PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-310387

(43)Date of publication of application : 04.11.2004

---

(51)Int.Cl. G06F 1/00
G06F 12/14
G06F 15/02
H04B 7/26
H04M 1/725
H04Q 7/38

---

(21)Application number : 2003-102346 (71)Applicant : SONY CORP

(22)Date of filing : 04.04.2003 (72)Inventor : TAJIMA SHIGERU

---

(54) AUTHENTICATION CONFIRMATION SYSTEM, AUTHENTICATION CONFIRMATION METHOD, AND PORTABLE INFORMATION PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication confirmation system capable of protecting secret information stored in a portable information processor based on a result of authentication confirmation.
SOLUTION: This authentication confirmation system 1 authenticates, when a battery pack 11 in the portable information processor 10 is charged with a charging apparatus 30, whether or not the charging is performed with the charging apparatus 30 connected to the portable information processor 10 at the time of initial setting by a valid user. As the result of authentication, when it is determined that the processor 10

is connected to a charging apparatus different from the charging apparatus 30 connected at the time of initial setting, or cannot be authenticated (rejection of authentication), the memory area of a memory in which personal and secret information are stored is erased.

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1]
A portable information processor which a control means performs information processing operation using electric power supplied from a rechargeable battery of cell housing bodies, and memorizes an individual and confidential information relevant to information processing to a memory measure,
Charging equipment which information about charge of said cell accommodation body is read, generates information for attestation, and charges said rechargeable battery,
It has means of signal communication which perform communication about attestation which followed said information for attestation between said control means in said charging equipment and said portable information processor,
An attestation confirming system protecting an individual and confidential information within said memory measure based on communication about attestation by said means of signal communication.
[Claim 2]
. Based on communication about said attestation by said means of signal communication, eliminate said individual within said memory measure, and a storage area of confidential information. And/or, the attestation confirming system according to claim 1 characterized by what said individual and confidential information which are memorized in said memory measure based on communication about said attestation by said means of signal communication are eliminated for after a cable/wireless

transmission to a specific external device.

[Claim 3]

Said means of signal communication are also performing communication about a charging state according to information about said charge between said charging equipment and said cell accommodation body, When it detects that said rechargeable battery was exhausted to a predetermined level according to communication about said charging state by said means of signal communication, The attestation confirming system according to claim 1, wherein said control means of said portable information processor protects said individual and confidential information by eliminating said individual within said memory measure, and a storage area of confidential information.

[Claim 4]

After removing after legitimate charge of said rechargeable battery by said charging equipment of the back said authentication result was normal, or from said charging means, said portable information processor starts a timer and in accordance with a predetermined set period, The attestation confirming system according to claim 1 eliminating said individual and confidential information after a cable/wireless transmission to a specific external device.

[Claim 5]

The attestation confirming system according to claim 4 characterized by eliminating said individual and confidential information after a cable/wireless transmission to a specific external device by functional operation specific after said predetermined set-period progress.

[Claim 6]

It has two or more said charging equipment which charges the each second cell of each cell housing bodies of said one or more portable information processors, The attestation confirming system according to claim 1, wherein said means of signal communication perform communication about attestation between said one or more portable information processors and said two or more charging equipment and said said one or more portable information processors protect an individual and confidential information within each memory measure based on said communication.

[Claim 7]

It has two or more said portable information processors with which the each second cell of cell housing bodies is charged with said one or more charging equipment, The attestation confirming system according to claim 1, wherein said means of signal communication perform communication about attestation between said two or more portable information processors and said one or more charging equipment and said two or more of said portable information processors protect an individual and confidential information within each memory measure based on said communication.

[Claim 8]

The attestation confirming system according to claim 1, 6, or 7 which connecting said

charging equipment to a communications network, and supervising by an external device.

[Claim 9]

A portable information processor which a control means performs information processing operation using electric power supplied from a rechargeable battery of cell housing bodies, and memorizes an individual and confidential information relevant to information processing to a memory measure, Charging equipment which information about charge of said cell accommodation body is read, generates information for attestation, and charges said rechargeable battery, It is the attestation check method in an attestation confirming system which has means of signal communication which perform communication about attestation which followed said information for attestation between said control means in said charging equipment and said portable information processor,

When said charging equipment and said portable information processor are connected including said means of signal communication and a trigger switch is operated by user,

An initialization setting-out process that said charging equipment and said portable information processor share said information for attestation by said charging equipment's generating said information for attestation, and transmitting to a control section of said portable information processor via said means of signal communication,

An information read-out process for attestation that said charging equipment reads said information for attestation from said portable information processor through said means of signal communication after said initialization setting-out process at the time of ** to which said portable information processor is once removed and is again connected from said charging equipment,

A collation process with which charging equipment compares whether said information for attestation read at said information read-out process for attestation agrees with information for attestation which was being kept in charging equipment,

An information-protection process of protecting an individual and confidential information within said said memory measure based on a result of said collation process

An attestation check method characterized by preparation ******.

[Claim 10]

A control means which performs information processing operation using electric power supplied from a rechargeable battery of cell housing bodies,

A memory measure which memorizes an individual and confidential information relevant to information processing by said control means,

It has a timer means which detects progress of a predetermined set period,

A portable information processor starting said timer means after said rechargeable battery is charged legitimately, and eliminating said confidential information after wireless transmission to a specific external device after predetermined set-period

progress.

[Claim 11]

A control means which performs information processing operation using electric power supplied from a rechargeable battery of cell housing bodies,

A memory measure which memorizes an individual and confidential information relevant to information processing by said control means,

It has a timer means which detects progress of a predetermined set period,

A portable information processor starting said timer means after detecting charge consumed quantity of said rechargeable battery and reaching a predetermined level, and eliminating said confidential information after wireless transmission to a specific external device after predetermined set-period progress.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

WERABURU type information processors, such as a clock type information processing terminal in which this invention built in rechargeable batteries, such as a lithium ion battery, Or portable information processors, such as a cellular phone and a SEMIWE rubble type information processor like a Personal Digital Assistant (Personal Digital Assistant:PDA), It is related with the attestation confirming system and portable information processor which perform an attestation check between the charging equipment which charges a rechargeable battery.

[0002]

[Description of the Prior Art]

Small portable information processors, such as WERABURU type information processors, such as a clock type information processor having rechargeable batteries, such as a lithium ion battery, or a cellular phone, a SEMIWE rubble type information processor like PDA, are used widely. These portable information processors have already had a network connection function.

The electronic banking etc. which use these are becoming common as throughput increases.

[0003]

It is how the user for whom becoming a big problem at this time is using these portable information processors checks that he is a legitimate user, or [that is,] how to perform personal authentication. Although easy methods for this include a password,

of course and it is widely used with the personal computer (Personal Computer:PC) etc., it is only with a password in ** that it is not perfect. Although advanced methods using a biometric sensor, such as a wearing user validation, are proposed in the WERABURU type information processor, collation by a fingerprint, etc. are commercialized and there is nothing still decisive. Like a cellular phone or PDA, about the portable information processor of the type which is not WERABURU fundamentally, personal authentication is still more difficult and also encounters a theft easily.

[0004]

Then, some measures [like] listed to below from the former have been taken. For example, the user authentication method and user authentication system in a portable data communications terminal are indicated by JP,2000-3336,A. One pair is constituted from a user authentication device and a portable data communications terminal, and the respectively common user code is made to store in a memory. And it checks performing radio and existing in the distance with which both can communicate by a user's login request or the timer management for every fixed time, between these two devices. Only when it existed in the distance with which both can communicate here, and a portable data communications terminal attests with it being in proper condition of use and attests with it being in this proper condition of use, it is the art of permitting access to the host computer from a portable data communications terminal.

[0005]

The art about the terminal user authentic method by a portable telephone, etc. is indicated by JP,2002-176492,A. A terminal unit and a portable telephone constitute a pair and the existence and the telephone number of connection of a portable telephone to the interface part for peripheral equipment connection with which the terminal unit was equipped are detected, When [whose a telephone number was not a thing of the portable telephone of the registered user of a terminal unit even if case or connected] the portable telephone is not connected, use of a terminal unit is made improper, It is the art which the portable telephone is connected, and makes use of a terminal unit good when a telephone number is a thing of said registered user's portable telephone. In order to make use of a terminal unit improper, a screen saver is started, for example and operation is made improper.

[0006]

The electronic formula theft arrester and the related method are indicated by the ** table No. 517487 [2000 to] gazette. The system which consists of an electronic device which operates by the electric power supply from a battery unit, and a battery charger which charges a battery unit is indicated. Memory storage is formed in the battery charger and the recognition code is memorized by the data input means by which external was carried out. This recognition code is sent to the storage parts

store in a battery pack at the time of charge. The recognition code memorized in the storage parts store of a battery unit is sent also to the storage parts store of an electronic device. An electronic device compares the recognition code sent from the battery unit with the code which oneself had memorized, and if it judges that the effective recognition code has been sent, a device will be enabled and will operate in the usual mode. However, if it judges that the invalid recognition code has been sent, the code in a battery unit will be eliminated and a device will be disabled electronically.

[0007]

[Patent documents 1]

JP,2000-3336,A

[Patent documents 2]

JP,2002-176492,A

[Patent documents 3]

** table 2000-517487

[0008]

[Problem(s) to be Solved by the Invention]

By the way, in a user authentication method and a system given in said patent documents 1, one pair must be constituted from a user authentication device and a portable data communications terminal, and they must always be possessed in the distance which can communicate. A user authentication device is always required for the portable data communications terminal side, and it is inconvenient in respect of a cellular phone. When a portable data communications terminal is lost, or when a theft is carried out, since confidential information, such as a user's mail address and information in connection with electronic banking, remains in the storage parts store in a device, for example, a malicious third party will see, and there is a possibility that it may be used improperly.

[0009]

A terminal unit and a portable telephone need to constitute a pair also from the art about the terminal user authentic method by a portable telephone given in said patent documents 2, etc. That is, a portable telephone is always required for the terminal unit side. Confidential information, such as a user's mail address and information in connection with electronic banking, remains in the storage parts store of a terminal unit too, and there is a possibility that it may be used improperly by the malicious third party.

[0010]

If it is in an electronic formula theft arrester and a related method given in said patent documents 3, It differs from said two indication art in that it is called connection between the charging equipment only at the time of charge, and an electronic device, Although the device which always serves as a pair is not needed, in an electronic device, confidential information, such as a user's mail address and information in

connection with electronic banking, remains too, and there is a possibility that it may be used improperly by the malicious third party.

[0011]

This invention is made in view of said actual condition, and aims at offer of the attestation confirming system which can protect the confidential information memorized in the portable information processor based on the result of an attestation check, the attestation check method, and a portable information processor.

[0012]

[Means for Solving the Problem]

In order that an attestation confirming system concerning this invention may solve said technical problem, a control means performs information processing operation using electric power supplied from a rechargeable battery of cell housing bodies, And a portable information processor which memorizes an individual and confidential information relevant to information processing to a memory measure, Charging equipment which information about charge of said cell accommodation body is read, generates information for attestation, and charges said rechargeable battery, Between said control means in said charging equipment and said portable information processor, it has means of signal communication which perform communication about attestation according to said information for attestation, and an individual and confidential information within said memory measure are protected based on communication about attestation by said means of signal communication.

[0013]

An attestation check method concerning this invention is provided with the following. A portable information processor which a control means performs information processing operation using electric power supplied from a rechargeable battery of cell housing bodies, and memorizes an individual and confidential information relevant to information processing to a memory measure in order to solve said technical problem. Charging equipment which information about charge of said cell accommodation body is read, generates information for attestation, and charges said rechargeable battery. It is the attestation check method in an attestation confirming system which has means of signal communication which perform communication about attestation which followed said information for attestation between said control means in said charging equipment and said portable information processor, When said charging equipment and said portable information processor are connected including said means of signal communication and a trigger switch is operated by user, An initialization setting-out process that said charging equipment and said portable information processor share said information for attestation by said charging equipment's generating said information for attestation, and transmitting to a control section of said portable information processor via said means of signal communication.

At the time of ** to which said portable information processor is once removed and is

again connected from said charging equipment after said initialization setting-out process. An information read-out process for attestation that said charging equipment reads said information for attestation from said portable information processor through said means of signal communication, A collation process with which charging equipment compares whether said information for attestation read at said information read-out process for attestation agrees with information for attestation which was being kept in charging equipment, and an information-protection process of protecting an individual and confidential information within said said memory measure based on a result of said collation process.

[0014]
A control means which performs information processing operation using electric power supplied from a rechargeable battery of cell housing bodies in order that a portable information processor concerning this invention may solve said technical problem, A memory measure which memorizes an individual and confidential information relevant to information processing by said control means, After having a timer means which detects progress of a predetermined set period and charging said rechargeable battery legitimately, said timer means is started and said confidential information is eliminated after wireless transmission to a specific external device after predetermined set-period progress.
[0015]
A control means which performs information processing operation using electric power supplied from a rechargeable battery of cell housing bodies in order that a portable information processor concerning this invention may solve said technical problem, A memory measure which memorizes an individual and confidential information relevant to information processing by said control means, After having a timer means which detects progress of a predetermined set period, detecting charge consumed quantity of said rechargeable battery and reaching a predetermined level, said timer means is started and said confidential information is eliminated after wireless transmission to a specific external device after predetermined set-period progress.
[0016]
Are in these this inventions and a portable information processor, WERABURU type information processors, such as a clock type information processing terminal having a rechargeable battery (battery charger), Or it is widely used as small portable equipment, such as a cellular phone and a SEMIWE rubble type information processor like a Personal Digital Assistant (Personal Digital Assistant:PDA).
[0017]
Electric power supplied from a rechargeable battery stored in a battery pack is used for a portable information processor, For example, information is processed in

electronic banking processing of network connection processing, telebrief processing, E-mail processing, word processing, image management processing, address book creation management processing, telephone number management processing, merchandise purchase by a network, a commodity transaction, etc., spreadsheet processing, database processing, etc. And an individual and confidential information, such as telephone records relevant to these information processing, a mail address, an important document, an important picture, an address book, a telephone number, electronic banking data, and an identification code further in connection with electronic banking, are memorized in a memory.

[0018]

Charging equipment has a memory connected to the processor B connected to a signal transduction part other than a general functional division, and this processor B. In this attestation confirming system, the processor B of charging equipment. A tap is attached to this signal wire for a signal wire currently used for communication of said charging information between charging equipment and a battery pack from the first, and it is used as a signal transduction part which performs communication about attestation between processors in charging equipment and a portable information processor. That is, the processor B from a communication result about attestation between charging equipment and a processor which are performed in a signal transduction part. It is checked whether whether a portable information processor is a device which a legitimate user owns, charging equipment, or a portable information processor is the system set up according to right combination. A memory has memorized an identification code (ID), a random number, etc. which are used for authenticating processing performed by the processor B.

[0019]

Thus, it is in an attestation confirming system and the processor B of charging equipment functions as an authenticating processing execution part. In anticipated use periodically charged with regular charging equipment, an attestation confirming system checks combination with charging equipment by ID of a portable information processor at every time, and continues holding a situation which a user customized.

[0020]

When a theft etc. charge with other charging equipment, all of an individual and confidential information are eliminated. When a legitimate user has done said erroneous connection, although an individual and confidential information are eliminated, they make reinitialization possible.

[0021]

Therefore, an attestation confirming system of this invention eliminates only ID like said patent documents 3, apparatus cannot be used for it, and does not carry out it, but eliminates a certain memory area, and protects an individual and confidential information.

[0022]
At the time of charge of a rechargeable battery in a battery pack performed at every several days or every day, fundamentally, since this attestation confirming system carries out an attestation check, Like said patent documents 1 and the patent documents 2, one pair can be constituted from a user authentication device and a portable data communications terminal, and time and effort that they must always be possessed in distance which can communicate can be saved.
[0023]
It is not connected to a state from which it separated from this attestation confirming system, i.e., charging equipment, but the portable information processor can eliminate a field of a memory where said individual and confidential information were memorized in the state where charge is not made as well as refusal of said attestation. When a rechargeable battery of a built-in battery pack is exhausted to a predetermined level (that is, dead battery), a memory area will be eliminated, if lapsed time is measured by a timer and specific lapsed time passes at the same time it urges charge. If a dead battery is caused, an individual and confidential information will be protected. It can prevent an individual and confidential information being misused by the 3rd malicious person etc. by this.
[0024]
It is in an attestation confirming system of this invention, and in a portable information processor, if a timer is set and the set period by this timer comes at the same time last ID is set up by connection with charging equipment, it will go into an alert state. In the alert state, a predetermined monitoring function is performed and a portable information processor performs the following operations according to control of a processor. First, a communication function is started and personal information, others, and different information from the time of factory shipments are transmitted to a mail address beforehand set up on PC. Then, a memory area of a memory which has memorized an individual and confidential information containing a set up mail address will be eliminated. By carrying out like this, an individual and confidential information of a portable information processor will be eliminated from a memory, or a memory will return at the time of factory shipments. Thereby, a portable information processor will be in a state of only a very fundamental function being performed or being able to perform only reinitialization setting out combined with charging equipment. That is, said individual and confidential information will be transmitted to PC which a history understands before elimination of a memory area. By a wireless communication means or network connection which used radio, it connects with PC and a portable information processor transmits said individual and confidential information.
[0025]
If it is in an attestation confirming system of this invention, It has two or more said charging equipment which charges the each second cell of each cell housing bodies of

said one or more portable information processors, Said means of signal communication perform communication about attestation between said one or more portable information processors and said two or more charging equipment, and said said one or more portable information processors protect an individual and confidential information within each memory measure based on said communication. It has two or more said portable information processors with which the each second cell of cell housing bodies is charged with said one or more charging equipment, Said means of signal communication perform communication about attestation between said two or more portable information processors and said one or more charging equipment, and said two or more of said portable information processors protect an individual and confidential information within each memory measure based on said communication.

[0026]

Thereby, two or more sets of charging equipment which can respond to one set of a portable information processor can be set up. It is also possible to set up two or more sets of a portable information processor and two or more sets of charging equipment as a group similarly.

[0027]

It is in an attestation confirming system concerning this invention, and it connects with a communications network and said charging equipment may be supervised by an external device. Since charging equipment serves as network correspondence, the internal adjustment can supervise it from other PCs connected to LAN etc. Then, by executing with PC a program which checks existence of charging equipment shows easily that charging equipment was removed from LAN etc. if charging equipment is made impossible [operation] when removed from LAN, a reuse in a theft etc. will be boiled markedly and will become troublesome. Of course, if connected to LAN etc. at all, protection of a password etc. starts and protection by a key code to a product is also easy. That is, a minimum charging function is given in hard as a charging equipment side, an authentication function is set up by software with PC more than it, and even if the 3rd malicious person obtains only charging equipment, it becomes possible easily to suppose that setting out is impossible. This divides a function of charging equipment further, makes storage possible and raises a barrier to an unauthorized use to a separate place.

[0028]

[Embodiment of the Invention]

Hereafter, it explains, referring to drawings for some embodiments of this invention. A 1st embodiment is provided with the following.

The portable information processor 10 which performs information processing operation by the electric power supply from the rechargeable batteries (battery charger) 12, such as a lithium ion battery which are the attestation confirming

systems 1 of composition of being shown in drawing 1, and was stored in the battery pack 11.
Charging equipment 30 which charges the rechargeable battery 12 in the battery pack 11.
The signal transduction part 50 which performs communication about attestation between the charging equipment 30 and the portable information processor 10.

[0029]
Since the portable information processor 10 is portable, variety-of-information processing which is later mentioned using the electric power by a rechargeable battery is performed. In performing variety-of-information processing, start a variety-of-information processing program by a processor, or, Power consumption becomes larger as a device is used with a natural thing, since display a processing result on a liquid crystal display (LCD), a sound is outputted from a loudspeaker or it communicates by connecting with a network. Therefore, it is necessary to charge the rechargeable battery in a battery pack with charging equipment frequently like every several days or every day.
[0030]
This attestation confirming system 1 attests whether it is that charge accomplishes between the charging equipment 30 connected to the portable information processor 10 at the time of initial setting by a legitimate user, when the battery pack 11 in the portable information processor 10 is charged by the charging equipment 30. If it is got blocked and the thing for which the portable information processor 10 is connected to charging equipment which is different in the charging equipment 30 connected at the time of initial setting as a result of attestation and which cannot attest becomes clear (refusal of attestation), the corresponding memory area of the memory which has memorized the individual and confidential information which are mentioned later will be eliminated.
[0031]
WERABURU type information processors, such as a clock type information processing terminal in which the portable information processor 10 contained the rechargeable battery (battery charger) 12, Or it is widely used as small portable equipment, such as a cellular phone and a SEMIWE rubble type information processor like a Personal Digital Assistant (Personal Digital Assistant:PDA).
[0032]
The electric power supplied from the rechargeable battery 12 stored in the battery pack 11 is used for the portable information processor 10, For example, information is processed in electronic banking processing of network connection processing, telebrief processing, E-mail processing, word processing, image management processing, address book creation management processing, telephone number

management processing, the merchandise purchase by a network, a commodity transaction, etc., spreadsheet processing, database processing, etc. And an individual and confidential information, such as the telephone records relevant to these information processing, a mail address, an important document, an important picture, an address book, a telephone number, electronic banking data, and an identification code further in connection with electronic banking, are memorized in a memory.

[0033]

For this reason, the battery pack 11 which can be stored enabling free attachment and detachment as the portable information processor 10 is shown in drawing 1, The processor 13 and the memory 14 used as a data storage part including said individual and confidential information which are generated or needed by information processing, It has the key operation section 17, the loudspeaker 18, the microphone 19, and the liquid crystal display (LCD) 20 which consist of a ten key connected to the interface 15 for network communication, the input-and-output (I/O) interface 16, and the I/O interface 16, or switches. The portable information processor 10 is faced performing said variety-of-information processing, A network connection processing program which takes out one by one and is executed by the processor 13, A telebrief processing program, an E-mail processing program, a word-processing program, An image management processing program, an address book creation management processing program, a telephone number management processing program, It also has the program memory 21 which stores the operating system (OS) program etc. as well as application programs, such as electronic banking processing programs, such as merchandise purchase, a commodity transaction, etc. by a network, a spreadsheet processing program, and a data base processing program.

[0034]

The charging equipment 20 is usually connected to commercial power by AC plug 31. AC/DC conversion carries out AC from commercial power, it is made the predetermined voltage of a direct current, and current, and the rechargeable battery 12 in the battery pack 11 is supplied. Charge is performed by connecting to the terminal for charge of the battery pack 11 (-) the - side line 33 which connects to the terminal for charge of the battery pack 11 (+) the + side line 32 connected to the terminal for charge (+), and is connected to the terminal for charge (-). Although a graphic display is omitted in the battery pack 11 here, the memory which has memorized the date of manufacture, the identification code of charging frequency and a battery pack, etc., and the processor are provided.

[0035]

The internal configuration of the charging equipment 30 is shown in drawing 2. With the AC->DC converter 34, AC supplied by AC plug 31 connected to commercial power is changed into DC of a predetermined value, and is supplied to the charge control part 35 and the processor A36. The charge control part 35 performs charge

control, such as restriction of current, and stabilization of voltage, for charge. The processor A36 is a processor which carries out control by the charge control part 35. . The processor A36 is performed between said processors of the battery pack 11 by the signal wire which is the signal transduction part 50 mentioned later. From the communication about charge, the charging information for the charging frequency of the rechargeable battery 12 and battery residue and other managements is read, and the charging time by the charge control part 35, the temporal change of a charge, etc. are controlled based on such charging information. These AC->DC converter 34, the charge control part 35, and the processor A36 are the general functional divisions 37 of the charging equipment 30.

[0036]

The charging equipment 30 has the processor B38 connected to the signal transduction part 50 other than said general functional division 37, and the memory 39 connected to this processor B38. In this attestation confirming system 1, the processor B38, A tap is attached to this signal wire for the signal wire currently used for communication of said charging information between the charging equipment 30 and the battery pack 11 from the first, and it is used as the signal transduction part 50 which performs communication about attestation between the processors 13 in the charging equipment 30 and the portable information processor 10. That is, the processor B38 from the communication result about attestation between the charging equipment 30 and the processor 13 which are performed in the signal transduction part 50. It is checked whether whether the portable information processor 10 is a device which a legitimate user owns, the charging equipment 30, or the portable information processor 10 is the system set up according to right combination. The memory 39 has memorized an identification code (ID), a random number, etc. which are used for the authenticating processing performed by the processor B38.

[0037]

The functional block diagram of the authenticating processing which the processor B38 performs is shown in drawing 3. It consists of the random number generation part 40, the authenticating processing execution part 41, the encryption section 42, the decoding part 43, and the trigger switch (initial-setting switch) part 44.

[0038]

In the memory 39, ROM39a and RAM(or flash memory)39b are provided. ROM39a sets ID and others (for example, the part number of charging equipment, a serial number, the date of manufacture, etc.) the first stage at the time of factory shipments. RAM39b memorizes the processing result of a processor. In the first setting out, the signal from ID and the random number generation device at the time of factory shipments is processed and memorized. Addition or EXOR may be simply sufficient as this processing in ID and the random number at the time of factory shipments, for example, and it may be made into the form which can read ID the first stage combining

ID and a random number.

[0039]

The authenticating processing execution part 41 is combined by processing which mentioned above initial ID stored in ROM39a in the memory 39 at the time of initial setting, and the random number generated in the random number generation part 40, and is sent to the encryption section 42. The encryption section 42 enciphers ID and a random number said first stage, lets the signal transduction part 50 pass, and sends it to the processor 13 in the portable information processor 10. This will share ID between the charging equipment 30 and the portable information processor 10 mutually the first stage. The outline of the authentication operation after initial setting is mentioned later.

[0040]

The decoding part 43 decodes the signal about the authenticating processing sent from the processor 13 in the portable information processor 10. Since the trigger switch 44 is a switch operated, for example at the time of initial setting or the below-mentioned erroneous connection by a legitimate user, it is desirable to have inconspicuous composition pressed with a nib etc. so that a use may not be known by the 3rd person. Of course, it is not necessary to write a name etc. in a case.

[0041]

The processor B38 which is in the charging equipment 30 and was shown in drawing 2 may be unified by the processor A36.

[0042]

The details of operation of the attestation confirming system 1 which explained composition until now and which consists of the portable information processor 10, the charging equipment 30, and the signal transduction part 50 are explained below.

[0043]

The attestation confirming system 1 attests whether it is that charge accomplishes between the charging equipment 30 connected to the portable information processor 10 at the time of initial setting by a legitimate user, when charging the battery pack 11 in the portable information processor 10 with the charging equipment 30. Personal authentication that it is whether it is that the portable information processor 10 is used by the legitimate user by this will be performed.

[0044]

Then, when it purchases, by a user, the portable information processor 10 and the charging equipment 30 currently prepared as the accessories are connected as a pair of a normal combination, and initial setting is performed.

[0045]

The portable information processor 10 and the charging equipment 30 with which it was equipped with the battery pack 11 are connected, and charge is started. If it will charge above to some extent after charge starting, initial setting will become possible,

continuing this initial charging.

[0046]

By monitoring communication with the signal wire (the signal transduction part 50 and common use) of the processor in the battery pack 11 and the charge control part 35 shows the situation whether the rechargeable battery 12 in the battery pack 11 was charged, so that initial setting was possible. Whether the battery was charged by the grade which can be initialization set up makes the charging equipment 30 recognize LED visually to a user by attachment, lighting of this LED, blink, etc.

[0047]

This initial setting is started when a user operates the trigger switch 44. That is, if the user who got to know having charged by LED presses the trigger switch 44 with a nib etc. so that it can initialize, initial setting will start. After purchasing the portable information processor 10 and the charging equipment 30, after a rechargeable battery is charged to some extent, if a user pushes the trigger switch 44, an initialization action will be performed, but it is in the state combined with the charging equipment 30, and does in this way because [of the following reasons].

[0048]

Considering sample exhibition in a store etc., charging first after factory shipments is not necessarily the last customer (user). Therefore, initial setting cannot be performed at the time of factory shipments. Since inconvenience will occur when the inferior goods of charging equipment are discovered after that if charging equipment and a portable information processor are made to correspond to the couple 1 at the time of factory shipments, initial setting cannot be performed at the time of factory shipments. The last customer is also declaration of intention of charging with specific charging equipment, and, thereby, defines the pair of charging equipment and a portable information processor. It also has a meaning of the reset to a factory-shipments time.

[0049]

Actual initial setting is performed that it is the following, when the processor B38 functions as the authenticating processing execution part 41 of drawing 3. If the trigger switch 44 is pushed, ID at the time of the factory shipments read from ROM39a in the memory 39 and the random number signal generated from the random number generation part 40 are added simply first, for example, and while memorizing this result to RAM39b, the encryption section 42 will be passed. The information for attestation which consists of ID enciphered by the encryption section 42 and a random number signal communicates to the processor 13 of the portable information processor 10 via the signal transduction part 50. The portable information processor 10 decodes said enciphered information for attestation, and stores it in an own memory. This will share ID between the charging equipment 30 and the portable information processor 10 mutually the first stage.

[0050]
It not only may add ID and the random number at the time of factory shipments, but as mentioned above, logical sum addition (EXOR) may be carried out, and generation of the information for attestation may be made into the form which can read ID the first stage combining ID and a random number.
[0051]
It is suitably chosen by the throughput of the goods used or a processor whether ID and a random number are used at this time. Since it is generated based on a random number and newest ID differs for every communication even if the same may be said of encryption and decryption and it omits a code/decoding, it is also read and there is no not much big meaning in self. However, since it will become easy to analyze about a protocol if encryption and decryption are omitted, of course, safety falls.
[0052]
The basic motion in use after initial setting is completed is explained. on of the portable information processor 10 is always [power supply] a principle. Therefore, foundations have always equipped with the battery pack 11. However, in processing information in network connection processing etc. of the actual condition which was mentioned above, as consumption of the power consumption of a rechargeable battery uses a device, it is more intense. For this reason, charge of the battery pack 11 by the charging equipment 30 is frequently performed like every several days or every day. About one month at the longest is assumed. It is realistic to equip charging equipment periodically with such a device, and to supply a power supply. In this attestation confirming system 1, after using this point positively and performing initial setting, whenever it is connected to the charging equipment 30, communication for attestation is performed, and new ID is set.
[0053]
Once, ID (referred to as ID1) set as the portable information processor 10 removed from the charging equipment 30 is memorized by the charging equipment 30. If the portable information processor 10 is again connected to the charging equipment 30 in this state, the charging equipment 30 will read ID1 of the portable information processor 10, and will compare it with ID1 which he has memorized. Here, if it agrees, new ID (ID2) will be generated and it will transmit to the portable information processor 10 using the signal transduction part 50. The portable information processor 10 receives new ID (ID2), and sets it to the memory of the processor 13. The portable information processor 10 will achieve the results of the personal authentication of being used by the legitimate user, with the charging equipment 30. The portable information processor 10 can perform normal information processing operation after charge. Normal information processing operation here is information processing operation in the state of remaining without eliminating said confidential information.

[0054]
In not agreeing on the other hand as a result of collation with IDX which the charging equipment 30 read from the portable information processor 10, and ID1 which he has memorized but differing, The charging equipment 30 sends a result that it cannot get blocked and attest to the processor 13 of the portable information processor 10 as a result of the purport that it does not agree via the signal transduction part 50. Then, the processor 13 judges that the portable information processor 10 is used by the theft etc. by the 3rd person who is not legitimate. And the processor 13 eliminates the specific memory area of the memory 14 relevant to said information processing which has memorized an individual and confidential information, such as telephone records, a mail address, an important document, an important picture, an address book, a telephone number, electronic banking data, and an identification code in connection with electronic banking, further. Thus, a specific memory area is a certain set-up field which covers the field or them in which the legitimate user stores an individual and confidential information. Or the processor 13 may initialize the memory 14 in the state at the time of factory shipments, when it judges that the portable information processor 10 is used by the 3rd person who is not legitimate.
[0055]
Procedure of the attestation confirming system 1 after initial setting was performed is made into a flow chart, and is shown in drawing 4. It is the procedure which the processor B38 of the charging equipment 30 performs, and is a procedure when functioning as the authenticating processing execution function 41. once said initial setting was completed and connection was canceled, the charging equipment 30 and the portable information processor 10 were connected further -- judging (it is YES at Step S1) -- it starts. It can be judged whether the charging equipment 30 and the portable information processor 10 were connected by monitoring the communication of said charging information performed by that between the charging equipment 50 and the battery pack 11. Here, the information for attestation currently treated should add the random number (RND) to ID.
[0056]
The processor B38 reads ID set as the portable information processor 10 via the signal transduction part 50 (Step S2). For example, it is initialization ID at the time of initialization setting out, and ID1 [last]. The charging equipment 30 is sharing the portable information processor 10 and ID at the time of the last connection from which the time of initialization setting out or a legitimate authentication result was obtained. Therefore, since self has also memorized initialization ID or ID1 [last], it is judged whether ID of a portable information processor is effective based on this (Step S3).
[0057]
If it judges that ID of a portable information processor is effective (it is YES at Step

S3), it will progress to step S4. In step S4, a random number (RND1) is read from the portable information processor 10. This should also be shared with the portable information processor 10 at the time of the last connection from which the time of initialization setting out or a legitimate authentication result was obtained. And it judges whether a random number (RND1) is effective at Step S5, and agrees with the random number which has memorized self, and if effective and it will judge (it is YES at Step S5), it will progress to Step S6.

[0058]

It means that the result of the personal authentication that the portable information processor 10 of a user with legitimate having been judged as YES at Step S5 is used was obtained. In Step S6, a new random number (RND2) is generated from the random number generation part 40, and it adds to ID, and stores in RAM39b. Of course, ID2 [new] is generated and ID2 and random number RND2 may be stored in RAM39b. This new random number (RND2) or ID2 and random number RND2 are transmitted to the processor 13 of the portable information processor 10 by the communication which used the signal transduction part 50.

[0059]

When it is judged as (NO) which has not agreed at Step S3 or Step S5 as a result of collation of ID or a random number (RND), or when it is judged that they are unset up ID and an unset up random number, it progresses to Step S8. In Step S8, the processor B38 sends a result that it cannot get blocked and attest to the processor 13 of the portable information processor 10 as a result of the purport that it does not agree by communication which used the signal transduction part 50. Then, the processor 13 judges that the portable information processor 10 is used by the theft etc. by the 3rd person who is not legitimate. By this the processor 13 of the portable information processor 10, The specific memory area of the memory 14 relevant to said information processing which has memorized an individual and confidential information, such as telephone records, a mail address, an important document, an important picture, an address book, a telephone number, electronic banking data, and an identification code in connection with electronic banking, further is eliminated.

[0060]

It is progressing to Step S8 also with the case where it is judged that they are unset up ID and an unset up random number, at Step S3 or Step S5 as a result of collation of ID or a random number (RND). This is a measure for the trial which the 3rd person is going to repeal ID or the random number of the portable information processor 10, and do out of the object of a system after said initial setting.

[0061]

Thus, when the battery pack 11 in the portable information processor 10 is charged by the charging equipment 30 as for the attestation confirming system 1, It attests whether it is that charge accomplishes between the charging equipment 30 connected

to the portable information processor 10 at the time of initial setting by a legitimate user, and personal authentication that it is whether it is that the portable information processor 10 is used by the legitimate user is performed. And said individual and confidential information can be protected based on an authentication result, and what those individuals and confidential information are used for the 3rd malicious person can be prevented.

[0062]

By the way, even if a legitimate user connects with other different charging equipment from the charging equipment which connected the portable information processor 10 at the time of initialization setting out accidentally, the specific memory area of the memory 14 which has memorized an individual and confidential information at Step S8 will be eliminated.

[0063]

It prepares for the erroneous connection by such a legitimate user, step S9 and Step S10 are prepared, and initialization setting out can be performed again. However, it becomes conditions that the trigger switch (initial-setting switch) 44 is operated by the user in step S9. As mentioned above, the trigger switch 44 is a switch of inconspicuous composition of being pressed with a nib etc., and is a switch which the operation purpose understands only by a legitimate user. Therefore, when the trigger switch 44 is pressed by the valid user and the initialization mode is chosen in step S9, it goes into initialization setting-out mode again. In Step S10, it goes into the initialization mode, and the charging equipment 30 uses the signal transduction part 50 for the portable information processor 10, and transmits ID from ROM39a to it. Then, RND2 is generated at Step S6 (Step S6), and it is bound to said ID, and is stored in the memory of the processor 13 of the portable information processor 10 (Step S7).

[0064]

Being in the attestation confirming system 1, the processor B38 of the charging equipment 30 performs procedure shown in drawing 4, and functions as the authenticating processing execution part 41. For this reason, by the anticipated use periodically charged with the regular charging equipment 30, the attestation confirming system 1. Combination with the charging equipment 30 is checked by ID of the portable information processor 10 at every time, and holding the situation (situation where the user's individual and confidential information were memorized) which the user customized is continued.

[0065]

When a theft etc. charge with other charging equipment, all of an individual and confidential information are eliminated. When the legitimate user has done said erroneous connection, although an individual and confidential information are eliminated, they make reinitialization possible.

[0066]

Drawing 5 is the composition of the signal transduction part 50 (communication wire) circumference of the hardware used for a 1st embodiment. The processor 36 in charging equipment and the processor (controller) 64 of battery pack 11 built-in are connected by the signal transduction part 50. Since the communication between the battery and charging equipment which are used for the camcorder etc. is permanent communication, bus-line composition may be impossible for it. In this case, it is necessary to consider it as a line type bus line by the wired OR shown, for example in drawing 5. Although this example explains a line type bus line, even if it is multiple wire system, of course, it is possible. What is connected to it considers that the bus-line method can take a high impedance state, and it does not interfere. A line type bus line of drawing 5 is composition which has required the power supply voltage Vcc for the collector and each processor of the switching transistors 62, 63, 65, and 66 via the load resistance 61. So to speak in this composition, the processor A36 in the charging equipment connected by the signal transduction part 50 and the processor 64 of battery pack 11 built-in are the present communication portions. The processor B38 of the charging equipment 30 and the processor 13 of the portable information processor 10 are the communication controller portions extended by this invention this time. The processor B38 is a processor added in the charging equipment 30. (Although repeated, the processor A36 and common use may be sufficient.) On the other hand, the processor 13 is a processor in the portable information processor 10, and the exchange of ID is performed by the communication which used the signal transduction part 50 between the processors B38.

[0067]

Drawing 6 is an example of signal aspect. Based on the timing of the timing pulse 71 outputted from the processor A36 (master processor) of the charging equipment 30, each processor determines the timing which outputs data. For example, according to the timing of the timing pulse 71, it outputs like [the processor A36 calls it the data 72, and / the processor B38] the data 73. This is fundamentally the same as a token ring method. 1 byte of data D is defined following the header pulse HP, and the composition of data serves as a packet of a suitable number of bytes, as the numerals 74 show. The data 72 and information required in 73 can be included by such a method.

[0068]

As shown in drawing 7 as a structure of a packet, the transmission source address 75, the transmission destination address 76, the data length 77, and the data 78 (the data 1 - data N) are minimum necessities, and may also contain an error correction code etc. in this. The broadcasting code is also defined as the transmission destination address 76 (for example, 0).

[0069]

The protocol between the charging equipment 30 and the portable information processor 10 is also explained briefly. As shown in drawing 8, the charger output 81 is

a broadcast signal which the charging equipment 30 (it is correctly considered as the processor A36 of drawing 5 by the master-processor; book embodiment of the charging equipment 30) generates at the time of communication standby. If the portable information processor 10 is connected to the charging equipment 30, it will monitor how many devices as for the portable information processor 10, are on the same bus line now by monitoring the periodic time of the timing pulse 71 shown in drawing 6, and its address will be set up (it is considered as the address 2). Although one device is fundamentally assumed to one charging equipment in this embodiment, it is explained sufficient [plurality] as a portable information processor. And a broth and charging equipment perform ID request 83 for the authentication demand 82 to this to charging equipment (the address 1 and assumption). In addition, communication according to the procedure currently described at the flow chart of drawing 4 is performed (it continues with 84 and 85), and refusal of attestation or attestation becomes clear. The memory storage defined by the inside of the apparatus side at the time of attestation refusal is eliminated.

[0070]

It is not connected to the state 30 from which it separated from this attestation confirming system 1, i.e., charging equipment, but the portable information processor 10 can eliminate the field of a memory where said individual and confidential information were memorized in the state where charge is not made as well as refusal of said attestation. When the rechargeable battery 12 of the built-in battery pack 11 is exhausted to a predetermined level (that is, dead battery), lapsed time is measured by a timer which is later mentioned at the same time it urges charge, and if specific lapsed time passes, said memory area will be eliminated. If a dead battery is caused, said individual and confidential information will be protected. It can prevent an individual and confidential information being misused by the 3rd malicious person etc. by this.

[0071]

By the way, after the last ID setting is completed in said confirmation authentication system 1 (a 1st embodiment), in within a time [a certain / fixed], information may be able to be read easily. Although it is generally realistic to use combination with a password, etc., it advances explanation, assuming a password to be what is broken. Therefore, if the portable information processor 10 encounters a theft immediately after setting up last ID (and this probability becomes high in the user who has charged periodically), it will not be protected until it causes a dead battery, but will be hard to attain the original purpose. it seems that safety for that was improved -- what is carried out is a 2nd embodiment.

[0072]

The composition of the attestation confirming system 90 used as a 2nd embodiment is shown in drawing 9. It becomes the portable information processor 100 and the

personal computer (PC) 110, for example from the network 92 like the Internet. Of course, the charging equipment 30 may be included. Since the portion including this charging equipment 30 is the same as that of the system 1 of said 1st embodiment, explanation is omitted here.

[0073]

The portable information processor 100 is the composition of having added the timer 101 and the Radio Communications Department 102 to each part shown in said drawing 1 further. The software by which software, such as application software stored in the program memory 21, is started by a timer takes the lead.

[0074]

The Radio Communications Department 102 constitutes the local Radio Communications Department from a predetermined band treating part, an RF processing section, and a local wireless communication antenna, and does radio of the data between PC110, for example. PC110 and communication which were provided with the telephone function according to the telephone protocol by the Internet like VpIP, and were similarly provided with the VpIP function via the access point (AP) 91 can also be performed.

[0075]

Wireless connection of the portable information processor 100 can be carried out to AP91 via network communication I/F15, and it can also be connected with PC110 through the Internet 92.

[0076]

The Internet 92 makes the broadband transmission (Broadband Transmission) possible by the spread of a broadband and high-speed communication lines now. The Internet is realized using an optical fiber, CATV (cable TV), radio, etc. Generally, the network consists of not less than 500k bps communication lines. Of course, a local area network (Local Area Network:LAN) may be used.

[0077]

PC110 has connected ROM113, RAM114, HDD115, and LCD controller 116 to CPU111 via bus (BUS)112, as composition is shown in drawing 10. The input-and-output (IO) part 118, the network interface (I/F) 122, and the Radio Communications Department 123 are connected to CPU111 via the bus 112. LCD117 has connected with LCD controller 116. The loudspeaker 119, the microphone 120, and the key operation section 121 are connected to the IO section 118.

[0078]

In the portable information processor 100, if the timer 101 is set and the set period by this timer 101 comes at the same time last ID is set up by connection with the charging equipment 30, it will go into an alert state. The following functions are supervised in the state of an alert.

(1) Access to the personal information field of a memory.

(2) Access to the document which the user drew up.
(3) Communication with the exterior (this communication is also included when the WEB browser is contained.) It is because personal information is used as a part of information on this communication. .
[0079]
On the contrary, about the next thing, it does not supervise at all. This is for suppressing the rise of cost by supervising reasonably.
(4) Reference of a clock function.
(5) Reference of a calculator function.
(6) Only creation of a new document.
[0080]
When the above-mentioned monitoring function is performed in the state of an alert, the portable information processor 100 performs the following operations according to control of the processor 13. First, network communication I/F15 and the communication function using the Radio Communications Department 102 are started, and personal information, others, and different information from the time of factory shipments are transmitted to the mail address beforehand set up on PC110. Then, the memory area of the memory 14 which has memorized the individual and confidential information containing a set up mail address will be eliminated. By carrying out like this, the individual and confidential information of the portable information processor 100 will be eliminated from the memory 14, or the memory 14 will return at the time of factory shipments. Thereby, the portable information processor 100 will be in the state of only a very fundamental function being performed or being able to perform only reinitialization setting out combined with the charging equipment 30.
[0081]
Two or more stages may be established about the evacuation and elimination of information using the timer 101. For example, when the information for electronic banking is eliminated in the first timeout (for example, one day), the mail address memorized in the next timeout (the 2nd day) is eliminated and it becomes on the 3rd, it is ** from which all the data is eliminated.
[0082]
It may carry out, because it only eliminates, without saving to PC110 as which started the communication function and the user specified data. It is eliminating also in the state (for example, based on a remote place, an obstacle, etc.) where it becomes impossible between PC110 or AP91 communicating the Radio Communications Department 102 of the portable information processor 100 or network communication I/F15.
[0083]
Since backup data is saved its PC110 even if it results in such a situation while a regular user uses it (it can carry out raw [of the unforeseen accident that data is lost

according to communication failure] as mentioned above), it can set up again. As a setting method, the restoration by the communication function prepared for the manual or the portable information processor or either is possible. Of course, when returning the backup data saved PC110 to the portable information processor 10, it may be made to perform authenticating processing between the portable information processor 10 and PC110. Also when this has crossed PC110 to the 3rd malicious person's hand, said individual and confidential information can be protected.

[0084]

By the way, with the attestation confirming systems 1 and 90 of said 1st and 2nd embodiments, the charging equipment 30 has stated only only one set of the case to the target portable information processors 10 and 100. Since establishment of a theft and loss also increases so much, safety is a translation raised in the thing with two or more sets to limit to only one set, but in the actual world, it may be told to an office and a house that he wants every one set of charging equipment, for example. The thing in consideration of such a case is a 3rd embodiment.

[0085]

The composition of the attestation confirming system 120 used as a 3rd embodiment is shown in drawing 11. It is an attestation confirming system using the composition which enables charge of one set of the portable information processor 125 with two or more sets, for example, two sets, of the charging equipment 121 and 122. Of course, three or more sets and at least about ten sets of charging equipment are possible. It is the point that this attestation confirming system 120 makes said target charging equipment 121 and two or more sets of arbitrary charging equipment other than 122 impossible [simple addition correspondence] to one set of the portable information processor 125 at the time of initial setting. Thereby, suitable charging equipment prevents being able to set to enabled correspondence afterwards.

[0086]

In drawing 11, the connectors 123 and 124 for performing communication between charging equipment using the signal transduction part 126a are prepared for the first set of the charging equipment 121, and the 2nd set of the charging equipment 122.

[0087]

Also in this attestation confirming system 120, initial setting by a user is required. Initial setting connects the charging equipment 121,122 to be used in the signal transduction part 126a using the connectors 123 and 124, and connects the portable information processor 125 with the charging equipment 122 in the signal transduction part 12b further, Setting up ID of the portable information processor 125 has the feature, sharing mutual ID. Initialization setting out is performed in this state. The next processing is performed in this initialization setting out.

(1) Clear the contents of the portable information processor 125 (equivalent to the time of factory shipments).

(2) ID (ID1) of the charging equipment 121 and ID (ID2) of the charging equipment 122 are memorized by the memory in the processor of the portable information processor 125 through the signal transduction part 126a and the signal transduction part 126b between each connector 123 and 124. The random number by which both were charging equipment 121,122 generated simultaneously is bound to ID of each charging equipment, and is memorized. That is, ID1+RNDA-1 and ID2+RNDB-1 are memorized by the portable information processor 125.

[0088]

Said RNDB-1 will be updated by RNDB-2, once it removes the portable information processor 125 from a system and connects with the charging equipment 122 further again. RNDB-2 becomes an identification key to the charging equipment 122 after this (of course, updated further.).

[0089]

Thus, licence setting out is attained to two or more arbitrary charging equipment by connecting all of the 3rd charging equipment and portable information processor of an embodiment that are due to be used in the attestation confirming system 120 at the time of initialization, and setting it as the basis of check of being in the same place as the same time zone.

[0090]

Therefore, to the portable information processor side, it means that the database by ID of usable charging equipment and the pair of the random number generated at the last corresponding to it was done.

[0091]

Two or more sets of the charging equipment which can respond to one set of a portable information processor can be set up with this method. It is also possible to set up two or more sets of a portable information processor and two or more sets of charging equipment as a group similarly.

[0092]

The attestation confirming systems 1, 90, and 120 of 1st, 2nd, and 3rd embodiments explained so far have described the measure against safety improvement only by the side of a portable information processor. Becoming unauthorized use impossible, if a portable information processor and charging equipment do not always come to hand in a pair did not take a measure in the charging equipment side, although it had become improvement in safety. Then, the system for aiming at improvement in safety to charging equipment is explained as a 4th embodiment.

[0093]

The composition of the attestation confirming system 130 of a 4th embodiment is shown in drawing 12. This attestation confirming system 130 has connected the charging equipment 30 to the local area networks (Local Area Network:LAN) 132, such as Ethernet (registered trademark), using the network connecting connector 131. The

charging equipment 30 has attached the MAC (Media Access Control) address to NIC (Network Interface Card) as a network address (NIC is used as the network connecting connector 131). Therefore, if the charging equipment 30 is connected to a power supply and the network connecting connector 131 is connected to LAN132, existence of the charging equipment 30 will be recognized by PC110 via LAN132.

[0094]

The charging equipment 30 has the network connecting connector 131, as mentioned above, and it gives the MAC Address to NIC. That is, since it is network correspondence, the internal adjustment can supervise from other PC110 connected to LAN132. Then, by executing in PC110 the program which checks existence of the charging equipment 30 shows easily that the charging equipment 30 was removed from LAN132. if charging equipment 30 is made impossible [operation] when removed from LAN132, the reuse in a theft etc. will be boiled markedly and will become troublesome. Of course, if connected to LAN132 at all, protection of a password etc. starts and protection by the key code to a product is also easy.

[0095]

Namely, in this attestation confirming system 130. A minimum charging function is given in hard as a charging equipment 30 side, an authentication function is set up by software (it supplies by CDROM etc.) more than it PC110, and even if the 3rd malicious person obtains only the charging equipment 30, it becomes possible easily to suppose that setting out is impossible. This divides the function of the charging equipment 30 further, makes storage possible and raises the barrier to an unauthorized use to a separate place.

[0096]

It may be made for PC110 to control the function of the charging equipment 30 via LAN132. For example, it is the function control which monitors whether the charging equipment 30 was connected with the portable information processor 10 connected at the time of initial setting, and a different portable information processor, and an attestation identification result that is, and stops charge of the charging equipment 30 in attestation refusal. When the charging equipment 30 is separated from a network or a main power supply, the ID setting function of the function as the authenticating processing execution part 41 by the processor B38, etc. may be reset. The reset ID setting function can be restored by again legitimate procedure, such as press of said trigger switch 44.

[0097]

[Effect of the Invention]

According to the attestation confirming system concerning this invention, communication about attestation can be performed between the control means in charging equipment and a portable information processor, and the individual and confidential information which are memorized in the portable information processor

based on the result of an attestation check can be protected.

[0098]

According to the attestation check method concerning this invention, communication about attestation can be performed between the control means in charging equipment and a portable information processor, and the individual and confidential information which are memorized in the portable information processor based on the result of an attestation check can be protected.

[0099]

Since according to the portable information processor concerning this invention a timer means is started and an individual and confidential information are eliminated after wireless transmission to a specific external device after predetermined set-period progress after a rechargeable battery is charged legitimately, the confidential information memorized in the portable information processor can be protected.

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the composition of the attestation confirming system 1 used as a 1st embodiment.

[Drawing 2]It is a block diagram showing the internal configuration of charging equipment.

[Drawing 3]It is a functional block diagram of the processor B of charging equipment.

[Drawing 4]It is a flow chart which shows the procedure of the attestation confirming system 1 after initial setting was performed.

[Drawing 5]It is a hardware-constitutions figure of the signal transduction part circumference of the attestation confirming system 1.

[Drawing 6]It is a timing chart which shows the gestalt of the signal which is the target of the communication performed in a signal transduction part.

[Drawing 7]It is a figure showing the packet structure of said signal.

[Drawing 8]It is a figure for explaining the protocol of said communication performed in a signal transduction part.

[Drawing 9]It is a block diagram showing the composition of the attestation confirming system 90 used as a 2nd embodiment.

[Drawing 10]It is a block diagram showing the internal configuration of a personal computer.

[Drawing 11]It is a block diagram showing the composition of the attestation confirming system 120 used as a 3rd embodiment.

[Drawing 12]It is a block diagram showing the composition of the attestation confirming system 130 used as a 4th embodiment.

[Description of Notations]

1 and 90,120,130 An attestation confirming system and 10,100,125 Portable information processor, 11 A battery pack and 12 A rechargeable battery and 13 A

processor and 14 Memory, 30,121,122 [A random number generation part and 41 / An authenticating processing execution part and 42 / An encryption section and 43 / A decoding part and 44 / A trigger switch and 50 / Signal transduction part] Charging equipment and 36 The processor A, the 38 processors B, and 39 A memory and 40

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-310387
(P2004-310387A)
(43)公開日　平成16年11月4日(2004.11.4)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 1/00	G06F	1/00	370E	5B017
G06F 12/14	G06F	12/14	320C	5B019
G06F 15/02	G06F	12/14	320D	5K027
H04B 7/26	G06F	15/02	335E	5K067
H04M 1/725	G06F	15/02	360Z	

審査請求 未請求　請求項の数 11　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願2003-102346(P2003-102346)
(22)出願日　平成15年4月4日(2003.4.4)

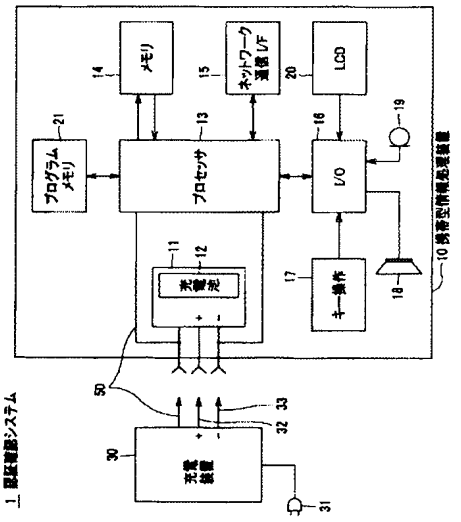
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100067736
弁理士　小池　晃
(74)代理人　100086335
弁理士　田村　榮一
(74)代理人　100096677
弁理士　伊賀　誠司
(72)発明者　田島　茂
東京都品川区東五反田３丁目１４番１３号
株式会社ソニーコンピュータサイエンス
研究所内

Ｆターム(参考)　5B017 AA07　BA08　CA14　CA16
5B019 CA04　GA10　KA10

最終頁に続く

(54)【発明の名称】認証確認システム及び認証確認方法並びに携帯型情報処理装置

(57)【要約】
【課題】認証確認の結果に基づいて携帯型情報処理装置内に記憶されている秘密情報を保護することのできる認証確認システムを提供する。
【解決手段】認証確認システム１は、携帯型情報処理装置１０内のバッテリパック１１が充電装置３０によって充電されるときに、正統なユーザによる初期設定時に携帯型情報処理装置１０に接続された充電装置３０との間で充電が成されるのか否かを認証する。認証の結果、携帯型情報処理装置１０が初期設定時に接続された充電装置３０とは異なる充電装置に接続されている、つまり認証できないことが判明すると（認証の拒否）、個人及び秘密情報を記憶しているメモリの該当メモリ領域を消去する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
電池収納体内の二次電池から供給される電力を用いて制御手段が情報処理動作を実行し、かつ情報処理に関連した個人及び秘密情報を記憶手段に記憶する携帯型情報処理装置と、前記電池収納体の充電に関する情報を読み取ると共に認証用情報を生成し、かつ前記二次電池を充電する充電装置と、
前記充電装置と前記携帯型情報処理装置内の前記制御手段との間で前記認証用情報にしたがった認証に関する通信を行う信号伝達手段とを有し、
前記信号伝達手段による認証に関する通信に基づいて前記記憶手段内の個人及び秘密情報を保護することを特徴とする認証確認システム。
【請求項２】
前記信号伝達手段による前記認証に関する通信に基づき前記記憶手段内の前記個人及び秘密情報の記憶領域を消去する、及び／又は前記信号伝達手段による前記認証に関する通信に基づいて前記記憶手段内に記憶されている前記個人及び秘密情報を特定の外部装置に有線／無線送信後、消去する、ことを特徴とする請求項１記載の認証確認システム。
【請求項３】
前記信号伝達手段は前記充電装置と前記電池収納体との間で前記充電に関する情報に応じた充電状態に関する通信も行っており、前記信号伝達手段による前記充電状態に関する通信に応じて前記二次電池が所定レベルまで消耗したことを検出したとき、前記携帯型情報処理装置の前記制御手段は前記記憶手段内の前記個人及び秘密情報の記憶領域を消去することによって前記個人及び秘密情報を保護することを特徴とする請求項１記載の認証確認システム。
【請求項４】
前記認証結果が正常であった後の前記充電装置による前記二次電池の正統な充電後、あるいは前記充電手段からの取り外し後に、前記携帯型情報処理装置はタイマーを起動し、所定設定時間経過により、前記個人及び秘密情報を特定の外部装置に有線／無線送信後、消去することを特徴とする請求項１記載の認証確認システム。
【請求項５】
前記所定設定時間経過後に特定の機能作動により、前記個人及び秘密情報を特定の外部装置に有線／無線送信後、消去することを特徴とする請求項４記載の認証確認システム。
【請求項６】
一つ以上の前記携帯型情報処理装置のそれぞれの電池収納体内の各二次電池を充電する前記充電装置を複数備えてなり、前記信号伝達手段は前記一つ以上の携帯型情報処理装置と前記複数の充電装置との間で認証に関する通信を行い、前記通信に基づいて前記一つ以上の前記携帯型情報処理装置は各記憶手段内の個人及び秘密情報を保護することを特徴とする請求項１記載の認証確認システム。
【請求項７】
一つ以上の前記充電装置によって電池収納体内の各二次電池が充電される前記携帯型情報処理装置を複数備えてなり、前記信号伝達手段は前記複数の携帯型情報処理装置と前記一つ以上の充電装置との間で認証に関する通信を行い、前記通信に基づいて前記複数の前記携帯型情報処理装置は各記憶手段内の個人及び秘密情報を保護することを特徴とする請求項１記載の認証確認システム。
【請求項８】
前記充電装置は通信網に接続し、外部の装置により監視されることを特徴とする請求項１、６又は７記載の認証確認システム。
【請求項９】
電池収納体内の二次電池から供給される電力を用いて制御手段が情報処理動作を実行し、かつ情報処理に関連した個人及び秘密情報を記憶手段に記憶する携帯型情報処理装置と、前記電池収納体の充電に関する情報を読み取ると共に認証用情報を生成し、かつ前記二次電池を充電する充電装置と、前記充電装置と前記携帯型情報処理装置内の前記制御手段と

の間で前記認証用情報にしたがった認証に関する通信を行う信号伝達手段とを有してなる認証確認システムにおける認証確認方法であって、
前記充電装置と前記携帯型情報処理装置とを前記信号伝達手段を含めて接続し、ユーザによりトリガースイッチが操作されたとき、前記充電装置は前記認証用情報を生成して前記信号伝達手段を介し、前記携帯型情報処理装置の制御部に送信することによって前記認証用情報を前記充電装置と前記携帯型情報処理装置にて共有する初期化設定工程と、
前記初期化設定工程後、前記充電装置から前記携帯型情報処理装置が一旦外され、再度接続されるたときに、前記充電装置が前記携帯型情報処理装置から前記信号伝達手段を通して前記認証用情報を読み出す認証用情報読み出し工程と、
前記認証用情報読み出し工程にて読み出した前記認証用情報が充電装置内に保管していた認証用情報と合致するか否かを充電装置が照合する照合工程と、
前記照合工程の結果に基づいて前記前記記憶手段内の個人及び秘密情報を保護する情報保護工程と
を備えることを特徴とする認証確認方法。
【請求項１０】
電池収納体内の二次電池から供給される電力を用いて情報処理動作を実行する制御手段と、
前記制御手段による情報処理に関連した個人及び秘密情報を記憶する記憶手段と、
所定設定時間の経過を検出するタイマー手段とを備え、
前記二次電池が正統に充電された後に、前記タイマー手段を起動し、所定設定時間経過後に、前記秘密情報を特定の外部装置に無線送信後、消去することを特徴とする携帯型情報処理装置。
【請求項１１】
電池収納体内の二次電池から供給される電力を用いて情報処理動作を実行する制御手段と、
前記制御手段による情報処理に関連した個人及び秘密情報を記憶する記憶手段と、
所定設定時間の経過を検出するタイマー手段とを備え、
前記二次電池の充電消耗量を検出し、所定レベルに達した後に、前記タイマー手段を起動し、所定設定時間経過後に、前記秘密情報を特定の外部装置に無線送信後、消去することを特徴とする携帯型情報処理装置。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、リチウムイオンバッテリー等の二次電池を内蔵した時計型情報処理端末等のウェラブル型情報処理装置、あるいは携帯電話や携帯情報端末（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ：ＰＤＡ）のようなセミウェラブル型情報処理装置等の携帯型情報処理装置と、二次電池を充電する充電装置との間で認証確認を行う認証確認システム並びに携帯型情報処理装置に関する。
【０００２】
【従来の技術】
リチウムイオンバッテリー等の二次電池を内蔵した時計型情報処理装置等のウェラブル型情報処理装置、あるいは携帯電話やＰＤＡのようなセミウェラブル型情報処理装置等の小型携帯型情報処理装置が広く使用されている。既に、これらの携帯型情報処理装置は、ネットワーク接続機能を有しており、処理能力が高まるにつれ、これらを使用した電子決済などが一般化してきている。
【０００３】
このときに大きな問題となるのが、それら携帯型情報処理装置を使用しているユーザが正統なユーザであることを如何にして確認するか、つまり個人認証をいかに行うかである。このための簡単な方法としてはもちろんパスワードがあり広くパーソナルコンピュータ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ：ＰＣ）等で使用されているが、パスワードだけで

は完全でないことは明かである。また、ウェラブル型の情報処理装置においてはバイオメトリックセンサーを用いての装着ユーザの確認等、高度な方式が提案されているが、商品化されているのは指紋による照合等でありまだまだ決定的なものはない。また、携帯電話やＰＤＡのように基本的にはウェラブルではないタイプの携帯型情報処理装置については、個人認証はさらに難しく、また盗難にも遭いやすい。

【０００４】

そこで、従来から以下に挙げるようないくつかの対策が採られてきた。例えば、特開２０００－３３３６号公報には、携帯型データ通信端末装置におけるユーザ認証方法及びユーザ認証システムが開示されている。ユーザ認証装置と携帯型データ通信端末装置とで一つのペアを構成し、それぞれ共通のユーザコードをメモリに格納させておく。そして、これら２つの装置間で、使用者のログイン要求や一定時間毎のタイマ管理によって無線通信を行い、両者が通信可能な距離に存在することを確認する。ここで、両者が通信可能な距離に存在すれば、携帯型データ通信端末装置が適正な使用状態にあると認証し、この適正な使用状態にあると認証した場合にだけ、携帯型データ通信端末装置からのホストコンピュータへのアクセスを許可する、という技術である。

【０００５】

また、特開２００２－１７６４９２号公報には、携帯電話機による端末ユーザ認証方式等に関する技術が開示されている。端末装置と携帯電話機によりペアを構成し、端末装置に備えられた周辺機器接続用インターフェース部への携帯電話機の接続の有無と電話番号とを検知し、携帯電話機が接続されていない場合、または接続されていても電話番号が端末装置の正規ユーザの携帯電話機のものでなかった場合には端末装置の使用を不可とし、携帯電話機が接続されており、かつ電話番号が前記正規ユーザの携帯電話機のものであった場合には端末装置の使用を可とする技術である。端末装置の使用を不可とするには、例えばスクリーンセーバを起動して操作を不可としている。

【０００６】

また、特表２０００－５１７４８７号公報には、電子式窃盗防止装置及び関連方法が開示されている。バッテリ・ユニットからの電力供給により動作する電子装置と、バッテリ・ユニットを充電する充電器とからなるシステムが開示されている。充電器にはメモリ記憶装置が設けられており、外付けされたデータ入力手段により承認コードを記憶している。この承認コードは、充電時にバッテリ・パック内の記憶部に送られる。また、バッテリ・ユニットの記憶部内に記憶された承認コードは、電子装置の記憶部にも送られる。電子装置は、バッテリ・ユニットから送られてきた承認コードと、自らが記憶していたコードとを比較し、有効な承認コードが送られてきたと判断すると、装置はイネーブルされ通常の態様で動作される。しかし、無効な承認コードが送られてきたと判断すると、バッテリー・ユニット内のコードを消去し、装置は電子的にディセーブルされる。

【０００７】

【特許文献１】

特開２０００－３３３６

【特許文献２】

特開２００２－１７６４９２

【特許文献３】

特表２０００－５１７４８７

【０００８】

【発明が解決しようとする課題】

ところで、前記特許文献１に記載のユーザ認証方法及びシステムでは、ユーザ認証装置と携帯型データ通信端末装置とで一つのペアを構成し、それらを通信可能な距離に常時所持しなければならない。携帯型データ通信端末装置の側には常にユーザ認証装置が必要であり、携帯という点では不便である。また、携帯型データ通信端末装置が紛失した場合、あるいは盗難された場合には、例えばユーザのメールアドレスや、電子決済に関わる情報等の秘密情報が装置内の記憶部に残ったままであるので悪意ある第三者に見られてしまうこ

とになり、不正使用される虞がある。
【０００９】
また、前記特許文献２に記載の携帯電話機による端末ユーザ認証方式等に関する技術でも、端末装置と携帯電話機によりペアを構成する必要がある。つまり、端末装置の側には携帯電話機が常に必要である。また、端末装置の記憶部にはやはり例えばユーザのメールアドレスや、電子決済に関わる情報等の秘密情報が残ってしまい、悪意ある第三者に不正使用される虞がある。
【００１０】
また、前記特許文献３に記載の電子式窃盗防止装置及び関連方法にあっては、充電時のみの充電装置と電子装置との接続という点では前記二つの開示技術とは異なり、常時ペアとなる装置を必要とすることはないが、電子装置内にはやはり例えばユーザのメールアドレスや、電子決済に関わる情報等の秘密情報が残ってしまい、悪意ある第三者に不正使用される虞がある。
【００１１】
本発明は、前記実情に鑑みてなされたものであり、認証確認の結果に基づいて携帯型情報処理装置内に記憶されている秘密情報を保護することのできる認証確認システム及び認証確認方法並びに携帯型情報処理装置の提供を目的とする。
【００１２】
【課題を解決するための手段】
本発明に係る認証確認システムは、前記課題を解決するために、電池収納体内の二次電池から供給される電力を用いて制御手段が情報処理動作を実行し、かつ情報処理に関連した個人及び秘密情報を記憶手段に記憶する携帯型情報処理装置と、前記電池収納体の充電に関する情報を読み取ると共に認証用情報を生成し、かつ前記二次電池を充電する充電装置と、前記充電装置と前記携帯型情報処理装置内の前記制御手段との間で前記認証用情報にしたがった認証に関する通信を行う信号伝達手段とを有し、前記信号伝達手段による認証に関する通信に基づいて前記記憶手段内の個人及び秘密情報を保護する。
【００１３】
本発明に係る認証確認方法は、前記課題を解決するために、電池収納体内の二次電池から供給される電力を用いて制御手段が情報処理動作を実行し、かつ情報処理に関連した個人及び秘密情報を記憶手段に記憶する携帯型情報処理装置と、前記電池収納体の充電に関する情報を読み取ると共に認証用情報を生成し、かつ前記二次電池を充電する充電装置と、前記充電装置と前記携帯型情報処理装置内の前記制御手段との間で前記認証用情報にしたがった認証に関する通信を行う信号伝達手段とを有してなる認証確認システムにおける認証確認方法であって、前記充電装置と前記携帯型情報処理装置とを前記信号伝達手段を含めて接続し、ユーザによりトリガースイッチが操作されたとき、前記充電装置は前記認証用情報を生成して前記信号伝達手段を介し、前記携帯型情報処理装置の制御部に送信することによって前記認証用情報を前記充電装置と前記携帯型情報処理装置にて共有する初期化設定工程と、前記初期化設定工程後、前記充電装置から前記携帯型情報処理装置が一旦外され、再度接続されるたときに、前記充電装置が前記携帯型情報処理装置から前記信号伝達手段を通して前記認証用情報を読み出す認証用情報読み出し工程と、前記認証用情報読み出し工程にて読み出した前記認証用情報が充電装置内に保管していた認証用情報と合致するか否かを充電装置が照合する照合工程と、前記照合工程の結果に基づいて前記前記憶手段内の個人及び秘密情報を保護する情報保護工程とを備える。
【００１４】
本発明に係る携帯型情報処理装置は、前記課題を解決するために、電池収納体内の二次電池から供給される電力を用いて情報処理動作を実行する制御手段と、前記制御手段による情報処理に関連した個人及び秘密情報を記憶する記憶手段と、所定設定時間の経過を検出するタイマー手段とを備え、前記二次電池が正統に充電された後に、前記タイマー手段を起動し、所定設定時間経過後に、前記秘密情報を特定の外部装置に無線送信後、消去する。

【００１５】
本発明に係る携帯型情報処理装置は、前記課題を解決するために、電池収納体内の二次電池から供給される電力を用いて情報処理動作を実行する制御手段と、前記制御手段による情報処理に関連した個人及び秘密情報を記憶する記憶手段と、所定設定時間の経過を検出するタイマー手段とを備え、前記二次電池の充電消耗量を検出し、所定レベルに達した後に、前記タイマー手段を起動し、所定設定時間経過後に、前記秘密情報を特定の外部装置に無線送信後、消去する。
【００１６】
これら本発明にあって、携帯型情報処理装置は、二次電池（充電池）を内蔵した時計型情報処理端末等のウェラブル型情報処理装置、あるいは携帯電話や携帯情報端末（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ：ＰＤＡ）のようなセミウェラブル型情報処理装置等の小型携帯型機器として広く使用されるものである。
【００１７】
携帯型情報処理装置は、バッテリーパック内に収納された二次電池から供給される電力を用いて、例えばネットワーク接続処理、電話通話処理、電子メール処理、文書作成処理、映像管理処理、住所録作成管理処理、電話番号管理処理、ネットワークによる商品購入及び商品取引等の電子決済処理、表計算処理、データベース処理等の情報処理を行う。そして、これらの情報処理に関連した、通話記録、メールアドレス、重要文書、重要画像、住所録、電話番号、電子決済データ、さらに電子決済に関わる識別コード等の個人及び秘密情報をメモリに記憶する。
【００１８】
充電装置は、一般的な機能部分の他に、信号伝達部に接続されるプロセッサＢと、このプロセッサＢに接続されるメモリを有する。この認証確認システムにおいて充電装置のプロセッサＢは、元々、充電装置とバッテリーパックとの間で前記充電情報の通信に使用されていた信号線を、この信号線にタップを付け、充電装置と携帯型情報処理装置内のプロセッサとの間の認証に関する通信を行う信号伝達部として使用する。つまり、プロセッサＢは、信号伝達部にて行われる充電装置とプロセッサとの間の認証に関する通信結果から、携帯型情報処理装置が正統なユーザの所有する装置であるか否か、又は充電装置と携帯型情報処理装置が正しい組み合わせにしたがって設定されたシステムであるか否かを確認する。メモリは、プロセッサＢにて行われる認証処理に用いられる識別コード（ＩＤ）や乱数等を記憶している。
【００１９】
このように、認証確認システムにあって充電装置のプロセッサＢは、認証処理実行部として機能する。認証確認システムは、定期的に正規の充電装置により充電する通常の使用では、そのたびに携帯型情報処理装置のＩＤにより充電装置との組み合わせをチェックし、ユーザがカスタマイズした状況を保持しつづける。
【００２０】
また、盗難等により、他の充電装置により充電された場合には、個人及び秘密情報はすべて消去される。もしも、正統なユーザが前記誤接続をしてしまったときには個人及び秘密情報は消去されるが、再初期設定を可能とする。
【００２１】
したがって、本発明の認証確認システムは、前記特許文献３のように単にＩＤだけを消去して機器を使えなくするのではなく、あるメモリ領域を消去して個人及び秘密情報を保護するものである。
【００２２】
また、この認証確認システムは、数日毎、あるいは毎日に行われるバッテリパック内の二次電池の充電時に基本的に、認証確認をするので、前記特許文献１及び特許文献２のように、ユーザ認証装置と携帯型データ通信端末装置とで一つのペアを構成し、それらを通信可能な距離に常時所持しなければならないという手間を省くことができる。
【００２３】

また、携帯型情報処理装置は、この認証確認システムから外れた状態、つまり充電装置に接続されず、充電がなされない状態でも、前記認証の拒否と同様に前記個人及び秘密情報の記憶されたメモリの領域を消去できる。内蔵されたバッテリーパックの二次電池が所定レベルまで消耗されたとき（つまりバッテリー切れ）には、充電を促すと同時にタイマーにて経過時間を計測し、特定の経過時間が過ぎたらメモリ領域を消去する。バッテリー切れを起こすと個人及び秘密情報を保護するわけである。これにより、悪意のある第３者等によって個人及び秘密情報が悪用されるのを防ぐことができる。

【００２４】

また、本発明の認証確認システムにあって携帯型情報処理装置では、充電装置との接続により最終ＩＤが設定されると同時にタイマーがセットされ、このタイマーによる設定時間になるとアラート状態に入る。アラート状態では所定の監視機能が実行され、携帯型情報処理装置はプロセッサの制御に応じて以下の動作を行う。先ず、通信機能を起動し、ＰＣ上に予め設定されたメールアドレスに対して個人情報その他、工場出荷時と異なる情報を送信する。このあと、設定済みのメールアドレスを含む個人及び秘密情報を記憶しているメモリのメモリ領域を消去してしまう。こうすることで、携帯型情報処理装置の個人及び秘密情報はメモリから消去されるか、あるいはメモリは工場出荷時に戻ってしまう。これにより携帯型情報処理装置は、ごく基本的な機能しかできないか、あるいは充電装置と組み合わせての再初期化設定しかできない等の状態になる。つまり、メモリ領域の消去の前に、素性の判っているＰＣに前記個人及び秘密情報を送信してしまう。携帯型情報処理装置は、無線通信手段により、または無線通信を用いたネットワーク接続により、ＰＣと接続し、前記個人及び秘密情報を送信するものである。

【００２５】

また、本発明の認証確認システムにあっては、一つ以上の前記携帯型情報処理装置のそれぞれの電池収納体内の各二次電池を充電する前記充電装置を複数備えてなり、前記信号伝達手段は前記一つ以上の携帯型情報処理装置と前記複数の充電装置との間で認証に関する通信を行い、前記通信に基づいて前記一つ以上の前記携帯型情報処理装置は各記憶手段内の個人及び秘密情報を保護する。また、一つ以上の前記充電装置によって電池収納体内の各二次電池が充電される前記携帯型情報処理装置を複数備えてなり、前記信号伝達手段は前記複数の携帯型情報処理装置と前記一つ以上の充電装置との間で認証に関する通信を行い、前記通信に基づいて前記複数の前記携帯型情報処理装置は各記憶手段内の個人及び秘密情報を保護する。

【００２６】

これにより、一台の携帯型情報処理装置に対応可能な複数台の充電装置が設定できる。また、同様に複数台の携帯型情報処理装置と複数台の充電装置をグループとして設定することも可能である。

【００２７】

また、本発明に係る認証確認システムにあって、前記充電装置は通信網に接続し、外部の装置により監視されてもよい。充電装置は、ネットワーク対応となっているため、その内部設定等が、ＬＡＮ等に接続された他のＰＣから監視できる。そこで、充電装置の存在をチェックするプログラムをＰＣにて実行することにより、充電装置がＬＡＮ等から取り外されたことは容易にわかる。また、充電装置をＬＡＮから外された時に動作不能としておけば、盗難等での再使用は格段に面倒になる。もちろん、ＬＡＮ等に接続される以上、パスワード等の保護がかかるし、製品に対するキーコードによる保護も容易である。すなわち、充電装置側として最低限の充電機能をハード的にもたせ、それ以上に認証機能はＰＣにてソフトウェア的に設定し、充電装置のみを悪意のある第３者が入手しても設定不能とすることが容易に可能となる。これは充電装置の機能をさらに分割し、別々の場所に保管可能とし、不正使用への障壁を高めるものである。

【００２８】

【発明の実施の形態】

以下、本発明のいくつかの実施の形態について図面を参照しながら説明する。第１の実施

の形態は、図１に示す構成の認証確認システム１であり、バッテリーパック１１内に収納したリチウムイオンバッテリー等の二次電池（充電池）１２からの電力供給により情報処理動作を実行する携帯型情報処理装置１０と、バッテリーパック１１内二次電池１２を充電する充電装置３０と、充電装置３０と携帯型情報処理装置１０との間で認証に関する通信を行う信号伝達部５０とを備えてなる。

【００２９】

携帯型情報処理装置１０は、携帯型であるため二次電池による電力を用いて後述するような各種情報処理を実行している。各種情報処理を行うにあたっては、プロセッサにより各種情報処理プログラムを起動したり、処理結果を液晶表示装置（ＬＣＤ）に表示したり、音声をスピーカから出力したり、あるいはネットワークに接続して通信を行うので当然のことながら装置を使えば使うほど電力消費量が大きくなる。よって、数日毎、あるいは毎日というように頻繁にバッテリパック内の二次電池を充電装置にて充電する必要がある。

【００３０】

この認証確認システム１は、携帯型情報処理装置１０内のバッテリパック１１が充電装置３０によって充電されるときに、正統なユーザによる初期設定時に携帯型情報処理装置１０に接続された充電装置３０との間で充電が成されるのか否かを認証する。認証の結果、携帯型情報処理装置１０が初期設定時に接続された充電装置３０とは異なる充電装置に接続されている、つまり認証できないことが判明すると（認証の拒否）、後述する個人及び秘密情報を記憶しているメモリの該当メモリ領域を消去する。

【００３１】

携帯型情報処理装置１０は、二次電池（充電池）１２を内蔵した時計型情報処理端末等のウェラブル型情報処理装置、あるいは携帯電話や携帯情報端末（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ：ＰＤＡ）のようなセミウェラブル型情報処理装置等の小型携帯型機器として広く使用される。

【００３２】

携帯型情報処理装置１０は、バッテリーパック１１内に収納された二次電池１２から供給される電力を用いて、例えばネットワーク接続処理、電話通話処理、電子メール処理、文書作成処理、映像管理処理、住所録作成管理処理、電話番号管理処理、ネットワークによる商品購入及び商品取引等の電子決済処理、表計算処理、データベース処理等の情報処理を行う。そして、これらの情報処理に関連した、通話記録、メールアドレス、重要文書、重要画像、住所録、電話番号、電子決済データ、さらに電子決済に関わる識別コード等の個人及び秘密情報をメモリに記憶する。

【００３３】

このため、携帯型情報処理装置１０は、図１に示すように、着脱自在に収納できるバッテリーパック１１と、プロセッサ１３と、情報処理によって生成或いは必要とされる前記個人及び秘密情報を含めたデータの記憶部として使われるメモリ１４と、ネットワーク通信用インターフェース１５と、入出力（Ｉ／Ｏ）インターフェース１６と、Ｉ／Ｏインターフェース１６に接続されるテンキーやスイッチ類からなるキー操作部１７，スピーカ１８，マイクロホン１９及び液晶表示装置（ＬＣＤ）２０を備える。さらに、携帯型情報処理装置１０は、前記各種情報処理を行うに際し、プロセッサ１３にて逐次取り出して実行されるネットワーク接続処理プログラム、電話通話処理プログラム、電子メール処理プログラム、文書作成処理プログラム、映像管理処理プログラム、住所録作成管理処理プログラム、電話番号管理処理プログラム、ネットワークによる商品購入及び商品取引等の電子決済処理プログラム、表計算処理プログラム、データベース処理プログラム等のアプリケーションプログラムはもちろん、オペレーティングシステム（ＯＳ）プログラム等を格納しているプログラムメモリ２１も備えている。

【００３４】

充電装置２０は、通常はＡＣプラグ３１により商用電源に接続される。商用電源からのＡＣをＡＣ／ＤＣ変換し、直流の所定の電圧、電流にしてバッテリーパック１１内の二次電池１２に供給する。充電用端子（＋）に接続されている＋側ライン３２をバッテリーパッ

ク１１の充電用端子（＋）に接続し、充電用端子（－）に接続されている－側ライン３３をバッテリーパック１１の充電用端子（－）に接続することによって充電が行われる。バッテリーパック１１には、ここでは図示を省略するが、製造年月日や充電回数、バッテリーパックの識別コード等を記憶しているメモリや、プロセッサが設けられている。

【００３５】

図２には、充電装置３０の内部構成を示す。商用電源に接続されたＡＣプラグ３１によって供給されたＡＣをＡＣ→ＤＣ変換器３４によって所定値のＤＣに変換し、充電制御部３５及びプロセッサＡ３６に供給する。充電制御部３５は、充電のために電流の制限や電圧の安定化等の充電制御を行う。プロセッサＡ３６は、充電制御部３５による制御を実施するプロセッサである。また、プロセッサＡ３６は、後述する信号伝達部５０である信号線によってバッテリーパック１１の前記プロセッサとの間で行われる、充電に関する通信から、二次電池１２の充電回数、電池残量その他管理のための充電情報を読み取り、これらの充電情報を基に充電制御部３５による充電時間や、充電量の時間変化等を制御する。これらＡＣ→ＤＣ変換器３４、充電制御部３５及びプロセッサＡ３６は、充電装置３０の一般的な機能部分３７である。

【００３６】

充電装置３０は、前記一般的な機能部分３７の他に、信号伝達部５０に接続されるプロセッサＢ３８と、このプロセッサＢ３８に接続されるメモリ３９を有する。この認証確認システム１においてプロセッサＢ３８は、元々、充電装置３０とバッテリーパック１１との間で前記充電情報の通信に使用されていた信号線を、この信号線にタップを付け、充電装置３０と携帯型情報処理装置１０内のプロセッサ１３との間の認証に関する通信を行う信号伝達部５０として使用する。つまり、プロセッサＢ３８は、信号伝達部５０にて行われる充電装置３０とプロセッサ１３との間の認証に関する通信結果から、携帯型情報処理装置１０が正統なユーザの所有する装置であるか否か、又は充電装置３０と携帯型情報処理装置１０が正しい組み合わせにしたがって設定されたシステムであるか否かを確認する。メモリ３９は、プロセッサＢ３８にて行われる認証処理に用いられる識別コード（ＩＤ）や乱数等を記憶している。

【００３７】

図３には、プロセッサＢ３８が行う認証処理の機能ブロック図を示す。乱数発生部４０と、認証処理実行部４１と、暗号化部４２と、復号部４３と、トリガースイッチ（初期設定スイッチ）部４４とからなる。

【００３８】

メモリ３９内には、ＲＯＭ３９ａとＲＡＭ（またはフラッシュメモリ）３９ｂが設けられている。ＲＯＭ３９ａは、初期ＩＤその他（例えば、充電装置の型番、シリアル番号、製造年月日等）を工場出荷時にセットする。ＲＡＭ３９ｂは、プロセッサの処理結果を記憶する。最初の設定においては工場出荷時のＩＤと乱数発生装置からの信号を処理し記憶する。この処理は、工場出荷時のＩＤと乱数を例えば単純に加算でも、ＥＸＯＲでもいいし、初期ＩＤと乱数を組み合わせて、ＩＤが読み出せるような形にしてもよい。

【００３９】

認証処理実行部４１は、初期設定時にメモリ３９内のＲＯＭ３９ａに格納されている初期ＩＤと乱数発生部４０で発生された乱数とを前述したような処理により組み合わせ、暗号化部４２に送る。暗号化部４２は、前記初期ＩＤと乱数とを暗号化し、信号伝達部５０を通して、携帯型情報処理装置１０内のプロセッサ１３に送る。これにより、充電装置３０と携帯型情報処理装置１０とで、互いに初期ＩＤを共有することになる。初期設定後の認証動作の概要について後述する。

【００４０】

復号部４３は、携帯型情報処理装置１０内のプロセッサ１３から送られてきた認証処理に関する信号を復号する。トリガースイッチ４４は、初期設定時、あるいは正統なユーザによる後述の誤接続時に例えば操作されるスイッチであるので、第３者に用途が知られないような、例えばペン先などで押圧される目立たない構成とするのが望ましい。もちろん、

筐体には名称等を書き入れる必要はない。
【００４１】
なお、充電装置３０にあって図２に示したプロセッサＢ３８は、プロセッサＡ３６に統合されていてもよい。
【００４２】
これまでに構成を説明した、携帯型情報処理装置１０と充電装置３０と信号伝達部５０からなる、認証確認システム１の動作の詳細について以下に説明する。
【００４３】
認証確認システム１は、携帯型情報処理装置１０内のバッテリパック１１を充電装置３０によって充電するときに、正統なユーザによる初期設定時に携帯型情報処理装置１０に接続された充電装置３０との間で充電が成されるのか否かを認証する。これにより、携帯型情報処理装置１０が正統なユーザによって使われるのか否かという個人認証が行われることになる。
【００４４】
そこで、購入した時点でユーザにより、携帯型情報処理装置１０とその付属品として用意されている充電装置３０とを、正常な組み合わせのペアとして接続し、初期設定を行う。
【００４５】
バッテリーパック１１が装着された携帯型情報処理装置１０と充電装置３０とを接続し、充電を開始する。充電開始後、ある程度以上充電された状態になったならば、この初期充電を続けながら、初期設定が可能となる。
【００４６】
初期設定が可能なほどにバッテリーパック１１内の二次電池１２が充電されたか否かの状況は、バッテリパック１１内のプロセッサと充電制御部３５との信号線（信号伝達部５０と共用）での通信を傍受することにより分かる。またバッテリが初期化設定可能程度に充電されたか否かは充電装置３０にＬＥＤを取付、このＬＥＤの点灯、点滅等によりユーザに視認させる。
【００４７】
この初期設定は、ユーザがトリガースイッチ４４を操作することにより開始する。つまり、初期設定可能なほどに充電されたのをＬＥＤにより知ったユーザがトリガースイッチ４４を例えばペン先などで押圧すると初期設定が始まる。携帯型情報処理装置１０と充電装置３０とを購入後、二次電池がある程度充電されたのち、充電装置３０と組み合わせた状態で、トリガースイッチ４４をユーザが押すと初期設定動作を行うわけであるが、このようにするのは、以下の理由のためである。
【００４８】
販売店等でのサンプル展示等を考えると、工場出荷後に最初に充電するのが最終カスタマー（ユーザ）とは限らない。よって、工場出荷時には初期設定は行えない。また、工場出荷時に充電装置と携帯型情報処理装置とを一対一に対応させると、その後に例えば充電装置の不良品が発見されたときに不都合が発生するので、工場出荷時には初期設定は行えない。また、最終カスタマーが特定の充電装置により充電するという意思表示でもあり、これにより充電装置と携帯型情報処理装置とのペアを定義する。また、工場出荷時点へのリセットという意味も持つ。
【００４９】
実際の初期設定は、プロセッサＢ３８が図３の認証処理実行部４１として機能することによって以下のよう行われる。トリガースイッチ４４が押されると、先ず、メモリ３９内のＲＯＭ３９ａから読み出した工場出荷時のＩＤと、乱数発生部４０から発生された乱数信号とを、例えば単純に加算し、この結果をＲＡＭ３９ｂに記憶するとともに暗号化部４２に渡す。暗号化部４２で暗号化されたＩＤと乱数信号からなる認証用情報は信号伝達部５０を介して携帯型情報処理装置１０のプロセッサ１３に通信される。携帯型情報処理装置１０は、前記暗号化された認証用情報を復号し、自身のメモリにストアする。これにより、充電装置３０と携帯型情報処理装置１０とで、互いに初期ＩＤを共有することになる。

【００５０】
なお、認証用情報の生成は、工場出荷時のＩＤと乱数とを加算するだけでなく、前述したように論理和加算（ＥＸＯＲ）してもよいし、初期ＩＤと乱数を組み合わせてＩＤが読み出せるような形にしてもよい。
【００５１】
このときにＩＤや乱数を使用するか否かは、使用される商品やプロセッサの処理能力によって適宜選択される。また暗号化、復号化についても同様で、もし暗号／復号を省略したとしても最新ＩＤは乱数に基づいて発生させられ、また通信毎に異なるので、読み取ってもこれ自身にはあまり大きな意味はない。ただし、暗号化、復号化を省略すると、プロトコルについては解析しやすくなるので、もちろん安全性は低下する。
【００５２】
初期設定が終了した後の、使用中の基本動作について説明する。携帯型情報処理装置１０は、電源常時ｏｎが原則である。よって、バッテリーパック１１は、常に装着しているのが基本である。しかし、前述したような現状のネットワーク接続処理等の情報処理を行うにあたっては、二次電池の消費電力の消耗は装置を使用すればするほど激しい。このため、充電装置３０によるバッテリーパック１１の充電は、数日毎、あるいは毎日というように頻繁に行われる。最長でも１ヶ月程度が想定される。このような装置では定期的に充電装置に装着して電源を補給しておくのが現実的である。この認証確認システム１では、この点を積極的に利用するものであり、初期設定が行われた後には、充電装置３０に接続される毎に認証用の通信を行い、新しいＩＤをセットする。
【００５３】
一度、充電装置３０から外された携帯型情報処理装置１０に設定されたＩＤ（ＩＤ１とする）は、充電装置３０にも記憶されている。この状態で、携帯型情報処理装置１０を充電装置３０に再度接続すると、充電装置３０は携帯型情報処理装置１０のＩＤ１を読み出し、自分が記憶しているＩＤ１と照合する。ここで、合致すれば新しいＩＤ（ＩＤ２）を生成し、信号伝達部５０を用いて携帯型情報処理装置１０に送信する。携帯型情報処理装置１０は、新しいＩＤ（ＩＤ２）を受け取りプロセッサ１３のメモリにセットしておく。充電装置３０によって携帯型情報処理装置１０は、正統なユーザによって使用されているという個人認証の結果を出すことになる。携帯型情報処理装置１０は、充電後に正常な情報処理動作を行うことができる。ここでいう正常な情報処理動作とは、前記秘密情報が消去されることなく残っている状態での情報処理動作である。
【００５４】
一方、充電装置３０が携帯型情報処理装置１０から読み出したＩＤＸと、自分が記憶しているＩＤ１との照合の結果、合致せず異なる場合には、充電装置３０は信号伝達部５０を介して合致しない旨の結果、つまり認証できないとの結果を携帯型情報処理装置１０のプロセッサ１３に送る。すると、プロセッサ１３は、携帯型情報処理装置１０が盗難等により正統でない第３者により使用されていると判断する。そして、プロセッサ１３は、前記情報処理に関連した、通話記録、メールアドレス、重要文書、重要画像、住所録、電話番号、電子決済データ、さらに電子決済に関わる識別コード等の個人及び秘密情報を記憶しているメモリ１４の特定のメモリ領域を消去する。このように、特定のメモリ領域とは、正統なユーザが個人及び秘密情報を格納している領域またはそれらをカバーするある設定された領域である。あるいは、プロセッサ１３は、携帯型情報処理装置１０が正統でない第３者によって使用されていると判断したときには、メモリ１４を工場出荷時の状態に初期化してもよい。
【００５５】
図４には、初期設定が行われた後の、認証確認システム１の処理手順をフローチャートにして示す。充電装置３０のプロセッサＢ３８が実行する処理手順であり、認証処理実行機能４１として機能するときの手順である。前記初期設定が終了し、一旦接続が解除された後、さらに充電装置３０と携帯型情報処理装置１０が接続されたことを判断する（ステップＳ１にてＹＥＳ）と始まる。充電装置３０と携帯型情報処理装置１０が接続されたか否

かは、充電装置５０とバッテリーパック１１間ので行われる前記充電情報の通信をモニタすることにより判断できる。なお、ここで、扱っている認証用情報は、ＩＤに乱数（ＲＮＤ）を加算したものとする。

【００５６】

プロセッサＢ３８は、信号伝達部５０を介して、携帯型情報処理装置１０に設定されたＩＤを読み出す（ステップＳ２）。例えば、初期化設定時の初期化ＩＤや、前回のＩＤ１である。充電装置３０は、初期化設定時或いは正統な認証結果が得られた前回の接続時には携帯型情報処理装置１０とＩＤを共有している。よって、自身も初期化ＩＤ又は前回のＩＤ１を記憶しているので、これを基に携帯型情報処理装置のＩＤが有効か否かを判断する（ステップＳ３）。

【００５７】

携帯型情報処理装置のＩＤが有効であると判断すると（ステップＳ３にてＹＥＳ）、ステップＳ４に進む。ステップＳ４では、乱数（ＲＮＤ１）を携帯型情報処理装置１０から読み出す。これも初期化設定時或いは正統な認証結果が得られた前回の接続時に、携帯型情報処理装置１０と共有しているはずである。そして、ステップＳ５にて乱数（ＲＮＤ１）が有効であるか否かを判断し、自身の記憶している乱数と合致し、有効であると判断（ステップＳ５にてＹＥＳ）したら、ステップＳ６に進む。

【００５８】

ステップＳ５にてＹＥＳと判断されたということは、正統なユーザの携帯型情報処理装置１０が使用されているという個人認証の結果が得られたことになる。ステップＳ６では、乱数発生部４０から新しい乱数（ＲＮＤ２）を発生し、ＩＤに加算してＲＡＭ３９ｂに格納する。もちろん、新しいＩＤ２を発生し、ＩＤ２と乱数ＲＮＤ２をＲＡＭ３９ｂに格納してもよい。この新しい乱数（ＲＮＤ２）、或いはＩＤ２と乱数ＲＮＤ２は、信号伝達部５０を用いた通信により携帯型情報処理装置１０のプロセッサ１３に送信される。

【００５９】

ステップＳ３又はステップＳ５にて、ＩＤ又は乱数（ＲＮＤ）の照合の結果、合致していない（ＮＯ）と判断した場合、或いは無設定ＩＤ、無設定乱数であると判断した場合は、ステップＳ８に進む。ステップＳ８において、プロセッサＢ３８は、信号伝達部５０を用いた通信によって合致しない旨の結果、つまり認証できないとの結果を携帯型情報処理装置１０のプロセッサ１３に送る。すると、プロセッサ１３は、携帯型情報処理装置１０が盗難等により正統でない第３者により使用されていると判断する。これにより、携帯型情報処理装置１０のプロセッサ１３は、前記情報処理に関連した、通話記録、メールアドレス、重要文書、重要画像、住所録、電話番号、電子決済データ、さらに電子決済に関わる識別コード等の個人及び秘密情報を記憶しているメモリ１４の特定のメモリ領域を消去する。

【００６０】

なお、ステップＳ３又はステップＳ５にて、ＩＤ又は乱数（ＲＮＤ）の照合の結果、無設定ＩＤ、無設定乱数であると判断した場合についても、ステップＳ８に進んでいる。これは、前記初期設定後に第３者が携帯型情報処理装置１０のＩＤ又は乱数を無効にしてシステムの対象外にしようとする試みに対する対策である。

【００６１】

このようにして、認証確認システム１は、携帯型情報処理装置１０内のバッテリパック１１が充電装置３０によって充電されるときに、正統なユーザによる初期設定時に携帯型情報処理装置１０に接続された充電装置３０との間で充電が成されるのか否かを認証し、携帯型情報処理装置１０が正統なユーザによって使われるのか否かという個人認証を行っている。そして、認証結果に基づいて前記個人及び秘密情報を保護することができ、それらの個人及び秘密情報が悪意の第３者に利用されるようなことを防ぐことができる。

【００６２】

ところで、正統なユーザが携帯型情報処理装置１０を初期化設定時に接続した充電装置とは異なる他の充電装置に誤って接続してしまってもステップＳ８にて個人及び秘密情報を

記憶しているメモリ１４の特定のメモリ領域は消去されてしまう。

【００６３】

このような正統なユーザによる誤接続に備え、ステップＳ９及びステップＳ１０が用意され、再度初期化設定を行うことができる。ただし、ステップＳ９にてトリガースイッチ（初期設定スイッチ）４４がユーザに操作されることが条件となる。トリガースイッチ４４は、前述したように、ペン先などで押圧される目立たない構成のスイッチであり、正統なユーザによってのみその操作目的が判るスイッチである。よって、ステップＳ９にて、正当なユーザによりトリガースイッチ４４が押圧されて初期設定モードが選択されたときには、再度初期化設定モードに入る。ステップＳ１０では、初期設定モードに入り、充電装置３０はＲＯＭ３９ａからのＩＤを携帯型情報処理装置１０に信号伝達部５０を用いて送信する。この後、ステップＳ６にてＲＮＤ２が発生され（ステップＳ６）、前記ＩＤにバインドされて携帯型情報処理装置１０のプロセッサ１３のメモリにストアされる（ステップＳ７）。

【００６４】

認証確認システム１にあって充電装置３０のプロセッサＢ３８は、図４に示した処理手順を実行して認証処理実行部４１として機能する。このため、認証確認システム１は、定期的に正規の充電装置３０により充電する通常の使用では、そのたびに携帯型情報処理装置１０のＩＤにより充電装置３０との組み合わせをチェックし、ユーザがカスタマイズした状況（ユーザの個人及び秘密情報が記憶された状況）を保持しつづける。

【００６５】

また、盗難等により、他の充電装置により充電された場合には、個人及び秘密情報はすべて消去される。もしも、正統なユーザが前記誤接続をしてしまったときには個人及び秘密情報は消去されるが、再初期設定を可能とする。

【００６６】

図５は第１の実施の形態に使用するハードウェアの信号伝達部５０（通信線）周辺の構成である。充電装置内のプロセッサ３６と、バッテリパック１１内蔵のプロセッサ（コントローラ）６４は、信号伝達部５０によって接続されている。カムコーダ等に使用されているバッテリーと充電装置間の通信は専用通信なので、バスライン構成が不可能な場合もありうる。この場合には、例えば図５に示すワイアードオアによる一線式バスラインとする必要がある。本実施例では一線式バスラインについて説明するが、多線式であってももちろん可能である。バスライン方式というのは、それに接続されるものがハイインピーダンス状態を取れるものと考えて差し支えない。図５の一線式バスラインは、負荷抵抗６１を介して電源電圧Ｖｃｃがスイッチングトランジスタ６２，６３，６５及び６６のコレクタ及び各プロセッサにかかっている構成である。この構成において、信号伝達部５０によって接続されている充電装置内のプロセッサＡ３６とバッテリパック１１内蔵のプロセッサ６４は、いわば現行の通信部分である。充電装置３０のプロセッサＢ３８と携帯型情報処理装置１０のプロセッサ１３が本発明によって今回拡張された通信コントローラ部分である。プロセッサＢ３８は、充電装置３０内に追加されたプロセッサである。（繰り返すが、プロセッサＡ３６と共用でもよい。）一方、プロセッサ１３は携帯型情報処理装置１０内のプロセッサで、ＩＤのやり取り等はプロセッサＢ３８との間の信号伝達部５０を用いた通信により実行される。

【００６７】

図６は信号形態の一例である。充電装置３０のプロセッサＡ３６（マスタープロセッサ）より出力されるタイミングパルス７１のタイミングに基づいて各プロセッサがデータを出力するタイミングを決める。例えばプロセッサＡ３６はデータ７２、プロセッサＢ３８はデータ７３という様にタイミングパルス７１のタイミングに合わせて出力する。これは、基本的にトークンリング方式と同じである。また、データの構成は、符号７４で示すように、ヘッダーパルスＨＰに続いて１バイトのデータＤが定義され、適当なバイト数のパケットとなる。このような方式でデータ７２や７３の中に必要な情報を含ませることができる。

【００６８】
パケットの構造としては図７に示すように、送信元アドレス７５、送信先アドレス７６、データ長７７、データ７８（データ１～データＮ）が最小限必要で、これにエラー訂正コード等を含んでもよい。送信先アドレス７６にはブロードキャストコードも定義しておく（例えば０）。
【００６９】
また、充電装置３０と携帯型情報処理装置１０間のプロトコルについても簡単に説明する。図８に示すように、チャージャ出力８１は、充電装置３０（正確には充電装置３０のマスタープロセッサ；本実施の形態では図５のプロセッサＡ３６とする）が通信スタンバイ時に発生するブロードキャスト信号である。充電装置３０に携帯型情報処理装置１０が接続されると、携帯型情報処理装置１０は図６に示したタイミングパルス７１の一周期間をモニタし、いくつの装置が現在同じバスライン上にいるかをモニタし、自分のアドレスを設定する（アドレス２とする）。この実施の形態では基本的に充電装置１つに対して装置１つを想定しているが、携帯型情報処理装置は複数でもよいとして説明する。そして充電装置（アドレス１と仮定）に対して認証要求８２をだし、充電装置はこれに対してＩＤ要求８３を行う。あとは、図４のフローチャートに記してある処理手順に従った通信が行われ（８４，８５と続く）、認証あるいは認証の拒否が判明する。認証拒否時には機器側内部で定義されたメモリー領域を消去する。
【００７０】
なお、携帯型情報処理装置１０は、この認証確認システム１から外れた状態、つまり充電装置３０に接続されず、充電がなされない状態でも、前記認証の拒否と同様に前記個人及び秘密情報の記憶されたメモリの領域を消去できる。内蔵されたバッテリーパック１１の二次電池１２が所定レベルまで消耗されたとき（つまりバッテリー切れ）には、充電を促すと同時に後述するようなタイマーにて経過時間を計測し、特定の経過時間が過ぎたら前記メモリ領域を消去する。バッテリー切れを起こすと前記個人及び秘密情報を保護するわけである。これにより、悪意のある第３者等によって個人及び秘密情報が悪用されるのを防ぐことができる。
【００７１】
ところで、前記確認認証システム１（第１の実施の形態）では、最終ＩＤ設定が完了してから、ある一定の時間内では情報が容易に読み出せることがある。なお、一般的にはパスワードとの組み合わせなどを、使用するのが現実的であるが、パスワードは破られるものと仮定して説明を進める。したがって、最終ＩＤが設定された直後に携帯型情報処理装置１０が盗難に遭うと（そして定期的に充電しているユーザほどこの確率が高くなる）、バッテリー切れを起こすまで保護されず、本来の目的が達成しにくい。そのための安全性を高めたようとするのが第２の実施の形態である。
【００７２】
図９には第２の実施の形態となる認証確認システム９０の構成を示す。携帯型情報処理装置１００と、パーソナルコンピュータ（ＰＣ）１１０と、例えばインターネットのようなネットワーク９２からなる。もちろん、充電装置３０を含めてもよい。この充電装置３０を含めた部分は、前記第１の実施の形態のシステム１と同様であるのでここでは説明を省略する。
【００７３】
携帯型情報処理装置１００は、前記図１に示した各部に、さらにタイマー１０１と、無線通信部１０２を追加した構成である。また、プログラムメモリ２１に格納されているアプリケーションソフト等のソフトウェアは、タイマーにより起動されるソフトウェアが中心となる。
【００７４】
無線通信部１０２は、例えばローカル無線通信部を、所定バンド処理部、ＲＦ処理部、ローカル無線通信アンテナで構成し、ＰＣ１１０との間でデータを無線通信する。また、ＶｐＩＰのようなインターネットによる電話プロトコルにしたがった電話機能を備え、アク

セスポイント（ＡＰ）９１を介して同じくＶｐＩＰ機能を備えたＰＣ１１０と通信を行うこともできる。

【００７５】

なお、携帯型情報処理装置１００は、ネットワーク通信Ｉ／Ｆ１５を介して、ＡＰ９１に無線接続し、インターネット９２を通してＰＣ１１０と接続することもできる。

【００７６】

インターネット９２は、現在、広帯域、高速な通信回線の普及によってブロードバンド伝送（Ｂｒｏａｄｂａｎｄ　Ｔｒａｎｓｍｉｓｓｉｏｎ）を可能としている。インターネットは、光ファイバーやＣＡＴＶ（ケーブルテレビ）、無線等を用いて実現されている。一般には、５００ｋｂｐｓ以上の通信回線でネットワークを構成している。もちろん、構内ネットワーク（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ：ＬＡＮ）を用いてもよい。

【００７７】

ＰＣ１１０は、図１０に構成を示すように、ＣＰＵ１１１にバス（ＢＵＳ）１１２を介して、ＲＯＭ１１３、ＲＡＭ１１４、ＨＤＤ１１５、ＬＣＤコントローラ１１６を接続している。また、ＣＰＵ１１１にバス１１２を介して入出力（ＩＯ）部１１８、ネットワークインターフェース（Ｉ／Ｆ）１２２、無線通信部１２３を接続している。ＬＣＤコントローラ１１６にはＬＣＤ１１７が接続している。また、ＩＯ部１１８には、スピーカ１１９、マイクロホン１２０や、キー操作部１２１が接続されている。

【００７８】

携帯型情報処理装置１００においては、充電装置３０との接続により、最終ＩＤが設定されると同時にタイマー１０１がセットされ、このタイマー１０１による設定時間になるとアラート状態に入る。アラート状態では次のような機能を監視する。

（１）メモリーの個人情報領域へのアクセス。

（２）ユーザが作成した文書へのアクセス。

（３）外部との通信（ＷＥＢブラウザが入っている場合にはこの通信も含む。個人情報がこの通信の情報の一部として使用されるためである。）。

【００７９】

逆に、以下に挙げるものについては全く監視しない。これは、監視をリーズナブルにすることによりコストの上昇を抑えるためである。

（４）時計機能の参照。

（５）電卓機能の参照。

（６）新規文書の作成のみ。

【００８０】

アラート状態で上記監視機能が実行された場合、携帯型情報処理装置１００はプロセッサ１３の制御に応じて以下の動作を行う。先ず、ネットワーク通信Ｉ／Ｆ１５や、無線通信部１０２を用いた通信機能を起動し、ＰＣ１１０上に予め設定されたメールアドレスに対して個人情報その他、工場出荷時と異なる情報を送信する。このあと、設定済みのメールアドレスを含む個人及び秘密情報を記憶しているメモリ１４のメモリ領域を消去してしまう。こうすることで、携帯型情報処理装置１００の個人及び秘密情報はメモリ１４から消去されるか、あるいはメモリ１４は工場出荷時に戻ってしまう。これにより携帯型情報処理装置１００は、ごく基本的な機能しかできないか、あるいは充電装置３０と組み合わせての再初期化設定しかできない等の状態になる。

【００８１】

なお、タイマー１０１を用いての情報の退避と消去については、複数の段階を設けてもよい。例えば、最初のタイムアウト（例えば１日）においては電子決済のための情報が消去され、次のタイムアウト（２日目）においては記憶しておいたメールアドレスが消去され、３日目になると全てのデータが消去される、等である。

【００８２】

さらに、通信機能を立ち上げてデータをユーザの指定したＰＣ１１０にセーブすることをせずに単に消去するだけにしてもよい。また、携帯型情報処理装置１００の無線通信部１

０２又はネットワーク通信Ｉ／Ｆ１５がＰＣ１１０又はＡＰ９１との間で通信不能となるような状態（例えば遠隔地、障害などによる）でも、消去するだけとなる。

【００８３】

仮に、正規のユーザが使用中にこのような事態に至っても、自分のＰＣ１１０にはバックアップデータが保存されているので（通信障害によりデータが無くなるという不慮の事故は前述したように生しうるが）、再度設定可能である。設定方法としては、マニュアルでも、携帯型情報処理装置に用意された通信機能による復旧でもどちらでも可能である。もちろん、ＰＣ１１０に保存されたバックアップデータを、携帯型情報処理装置１０に戻すときには、携帯型情報処理装置１０とＰＣ１１０との間で認証処理を行うようにしてもよい。これにより、ＰＣ１１０も悪意のある第３者の手に渡ってしまっていた場合にも、前記個人及び秘密情報を保護することができる。

【００８４】

ところで、前記第１及び第２の実施の形態の認証確認システム１及び９０では、対象とする携帯型情報処理装置１０及び１００に対して充電装置３０がただ一台のみの場合について述べてきた。複数台あればそれだけ盗難、紛失の確立も高まるので、ただ一台に限定することで安全性は高められる訳であるが、実社会においては、例えばオフィスと自宅に一台ずつの充電装置が欲しいということもある。このような場合を考慮したものが第３の実施の形態である。

【００８５】

図１１には第３の実施の形態となる認証確認システム１２０の構成を示す。一台の携帯型情報処理装置１２５を、複数台例えば２台の充電装置１２１、１２２で充電可能とする構成を利用した認証確認システムである。もちろん、充電装置は３台以上、１０数台でも可能である。この認証確認システム１２０は、一台の携帯型情報処理装置１２５に対して初期設定時に対象とした前記充電装置１２１、１２２以外の任意の複数台の充電装置を単純追加対応不能とすることがポイントである。これにより、適当な充電装置が後から対応可能に設定できてしまうのを防ぐ。

【００８６】

図１１において、一台目の充電装置１２１と、２台目の充電装置１２２には、充電装置間の通信を信号伝達部１２６ａを用いて実行するためのコネクタ１２３、１２４が用意されている。

【００８７】

この認証確認システム１２０においてもユーザによる初期設定が必要である。初期設定は、使用する充電装置１２１，１２２をコネクタ１２３、１２４を用いて信号伝達部１２６ａで接続し、さらに信号伝達部１２ｂにて携帯型情報処理装置１２５を充電装置１２２で接続して、お互いのＩＤを共有しながら携帯型情報処理装置１２５のＩＤを設定することに特徴がある。この状態で初期化設定が行われる。この初期化設定では次の処理が実行される。

（１）携帯型情報処理装置１２５の内容をクリア（工場出荷時と同等）する。

（２）充電装置１２１のＩＤ（ＩＤ１）、充電装置１２２のＩＤ（ＩＤ２）が各コネクタ１２３、１２４間の信号伝達部１２６ａ、及び信号伝達部１２６ｂを通して携帯型情報処理装置１２５のプロセッサ内のメモリに記憶される。同時に両方の充電装置１２１，１２２ら発生された乱数が各充電装置のＩＤにバインドされて記憶される。つまり、携帯型情報処理装置１２５にはＩＤ１＋ＲＮＤＡ－１及びＩＤ２＋ＲＮＤＢ－１が記憶される。

【００８８】

一旦、携帯型情報処理装置１２５をシステムから外し、さらに再度充電装置１２２に接続すると、前記ＲＮＤＢ－１はＲＮＤＢ－２に更新される。ＲＮＤＢ－２はこれ以降の充電装置１２２に対しての識別キーとなる（もちろん、更に更新される。）。

【００８９】

このように、第３の実施の形態の認証確認システム１２０では、初期化時に使用予定の充電装置と携帯型情報処理装置を全て接続し、同じ時間帯に同じ場所にあるという確認のも

とに設定することにより、任意の複数の充電装置に対して使用許可設定が可能になる。
【００９０】
したがって、携帯型情報処理装置側には使用可能な充電装置のＩＤとそれに対応する最後に発生された乱数のペアによるデータベースが出来上がったことになる。
【００９１】
この方式により一台の携帯型情報処理装置に対応可能な複数台の充電装置が設定できる。また、同様に複数台の携帯型情報処理装置と複数台の充電装置をグループとして設定することも可能である。
【００９２】
これまで説明してきた第１、第２及び第３の実施の形態の認証確認システム１、９０及び１２０では、携帯型情報処理装置側のみの安全性向上対策について述べてきた。常に携帯型情報処理装置と充電装置をペアで入手しないと不正使用不能になるというのは、安全性の向上にはなっているが、充電装置側では対策を採ってこなかった。そこで、充電装置に対する安全性向上を図るためのシステムを第４の実施の形態として説明する。
【００９３】
図１２には第４の実施の形態の認証確認システム１３０の構成を示す。この認証確認システム１３０は、充電装置３０をネットワーク接続コネクタ１３１を用いてイーサネット（登録商標）などの構内ネットワーク（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ：ＬＡＮ）１３２に接続している。充電装置３０は、ネットワークアドレスとしてＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスをＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）に付けている（ＮＩＣはネットワーク接続コネクタ１３１として用いている）。したがって、充電装置３０を電源に接続し、ネットワーク接続コネクタ１３１をＬＡＮ１３２に接続すると、充電装置３０の存在がＬＡＮ１３２を介して例えばＰＣ１１０に認識される。
【００９４】
充電装置３０は、前述したようにネットワーク接続コネクタ１３１を有し、ＮＩＣにＭＡＣアドレスを付している。つまり、ネットワーク対応となっているため、その内部設定等が、ＬＡＮ１３２に接続された他のＰＣ１１０から監視できる。そこで、充電装置３０の存在をチェックするプログラムをＰＣ１１０にて実行することにより、充電装置３０がＬＡＮ１３２から取り外されたことは容易にわかる。また、充電装置３０をＬＡＮ１３２から外された時に動作不能としておけば、盗難等での再使用は格段に面倒になる。もちろん、ＬＡＮ１３２に接続される以上、パスワード等の保護がかかるし、製品に対するキーコードによる保護も容易である。
【００９５】
すなわち、この認証確認システム１３０では、充電装置３０側として最低限の充電機能をハード的にもたせ、それ以上に認証機能はＰＣ１１０にてソフトウェア的に（ＣＤＲＯＭなどで供給）設定し、充電装置３０のみを悪意のある第３者が入手しても設定不能とすることが容易に可能となる。これは充電装置３０の機能をさらに分割し、別々の場所に保管可能とし、不正使用への障壁を高めるものである。
【００９６】
なお、ＰＣ１１０は、ＬＡＮ１３２を介して充電装置３０の機能を制御するようにしてもよい。例えば、充電装置３０が初期設定時に接続された携帯型情報処理装置１０と異なる携帯型情報処理装置と接続されたか否か、つまり認証確認結果をモニタし、認証拒否の場合には充電装置３０の充電を停止させるような機能制御である。また、充電装置３０がネットワーク又は主電源から切り離されたときには、プロセッサＢ３８による、認証処理実行部４１としての機能のＩＤ設定機能等をリセットしてもよい。リセットされたＩＤ設定機能は、前記トリガースイッチ４４の押圧等の再度正統な手続により復旧できる。
【００９７】
【発明の効果】
本発明に係る認証確認システムによれば、充電装置と携帯型情報処理装置内の制御手段と

の間で認証に関する通信を行い、認証確認の結果に基づいて携帯型情報処理装置内に記憶されている個人及び秘密情報を保護することができる。

【００９８】

本発明に係る認証確認方法によれば、充電装置と携帯型情報処理装置内の制御手段との間で認証に関する通信を行い、認証確認の結果に基づいて携帯型情報処理装置内に記憶されている個人及び秘密情報を保護することができる。

【００９９】

本発明に係る携帯型情報処理装置によれば、二次電池が正統に充電された後に、タイマー手段を起動し、所定設定時間経過後に、個人及び秘密情報を特定の外部装置に無線送信後、消去するので、携帯型情報処理装置内に記憶されている秘密情報を保護することができる。

【図面の簡単な説明】

【図１】第１の実施の形態となる認証確認システム１の構成を示すブロック図である。

【図２】充電装置の内部構成を示すブロック図である。

【図３】充電装置のプロセッサＢの機能ブロック図である。

【図４】初期設定が行われた後の、認証確認システム１の処理手順を示すフローチャートである。

【図５】認証確認システム１の信号伝達部周辺のハードウェア構成図である。

【図６】信号伝達部にて行われる通信の対象となる信号の形態を示すタイミングチャートである。

【図７】前記信号のパケット構造を示す図である。

【図８】信号伝達部にて行われる前記通信のプロトコルを説明するための図である。

【図９】第２の実施の形態となる認証確認システム９０の構成を示すブロック図である。

【図１０】パーソナルコンピュータの内部構成を示すブロック図である。

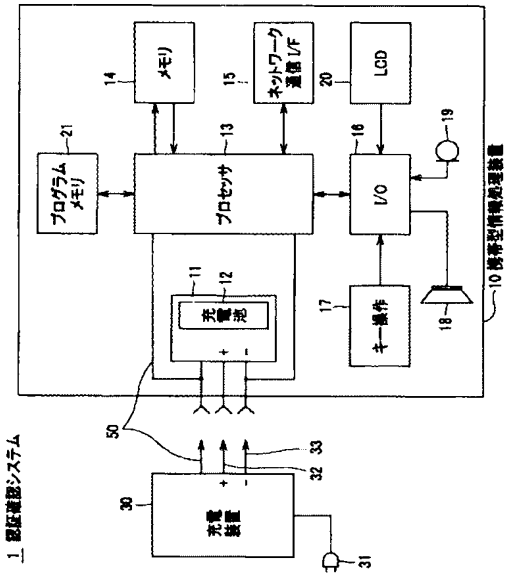
【図１１】第３の実施の形態となる認証確認システム１２０の構成を示すブロック図である。

【図１２】第４の実施の形態となる認証確認システム１３０の構成を示すブロック図である。

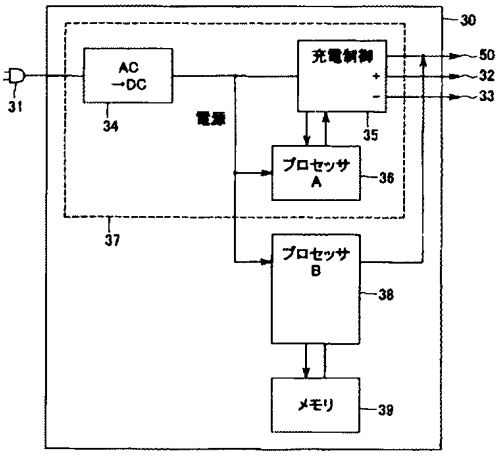
【符号の説明】

１，９０，１２０，１３０　認証確認システム、１０，１００，１２５　携帯型情報処理装置、１１　バッテリーパック、１２　二次電池、１３　プロセッサ、１４　メモリ、３０，１２１，１２２　充電装置、３６　プロセッサＡ、３８プロセッサＢ、３９　メモリ、４０　乱数発生部、４１　認証処理実行部、４２　暗号化部、４３　復号部、４４　トリガースイッチ、５０　信号伝達部

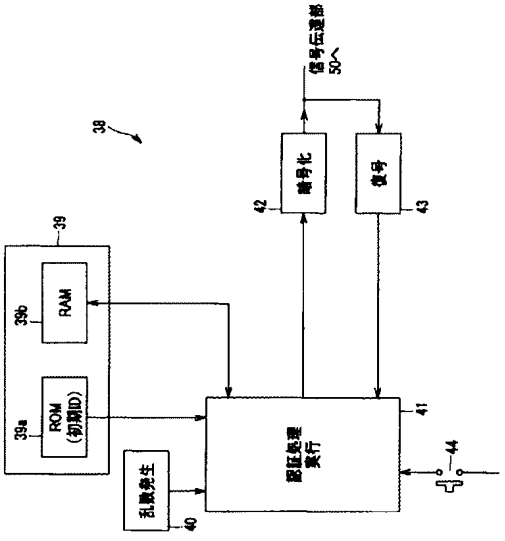
【図１】


1 認証確認システム
10 携帯型情報処理装置
メモリ
ネットワーク通信I/F
LCD
プログラムメモリ
プロセッサ
I/O
充電池
キー操作
充電装置

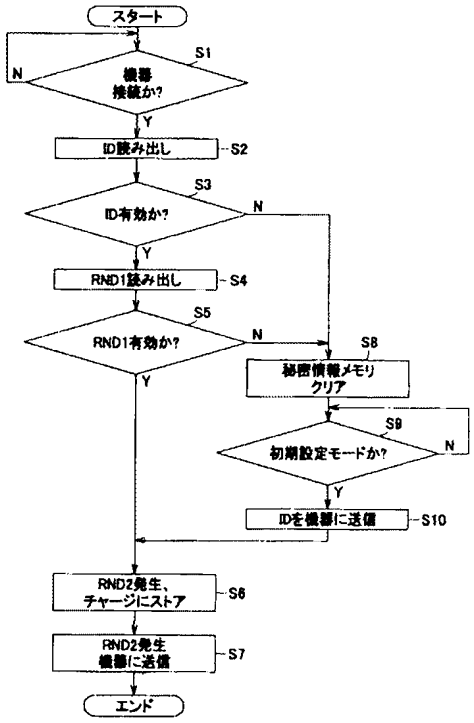
【図２】


AC→DC
充電制御
電源
プロセッサA
プロセッサB
メモリ

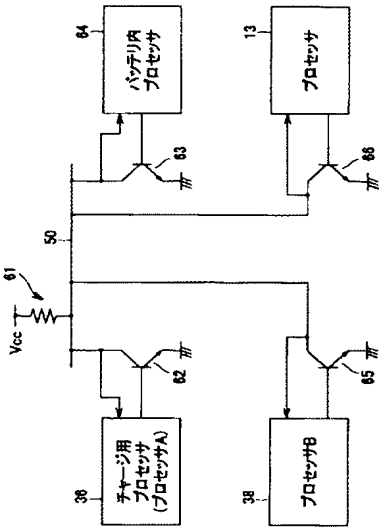
【図３】


信号伝達部
暗号化
復号
RAM
ROM（初期ID）
認証処理実行
乱数発生

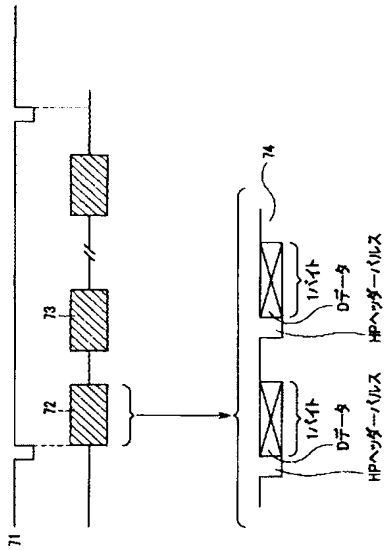
【図４】


スタート
機器接続か?
ID読み出し
ID有効か?
RND1読み出し
RND1有効か?
秘密情報メモリクリア
初期設定モードか?
IDを機器に送信
RND2発生、チャージにストア
RND2発生機器に送信
エンド

【図５】


64
バッテリ内プロセッサ
13
プロセッサ
63
66
50
61
Vcc
62
65
チャージ用プロセッサ(プロセッサA)
プロセッサB
36
38

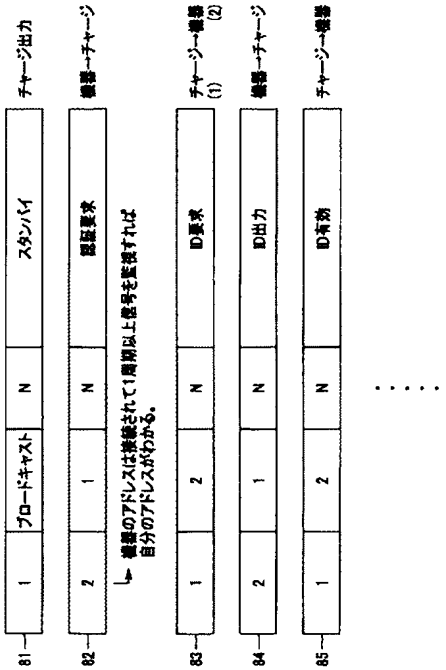
【図６】


74
73
72
71
1バイト
Dデータ
HPヘッダーパルス
1バイト
Dデータ
HPヘッダーパルス

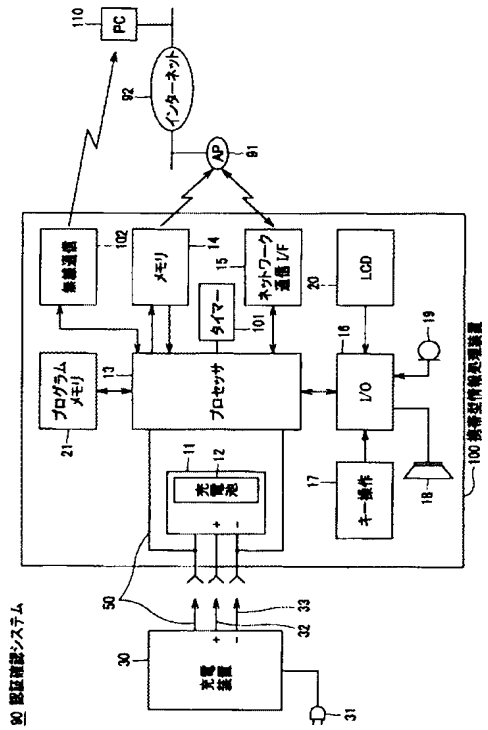
【図７】


78
77
76
75
送信元
送信先
データ長
データ1
・・・・・
データN

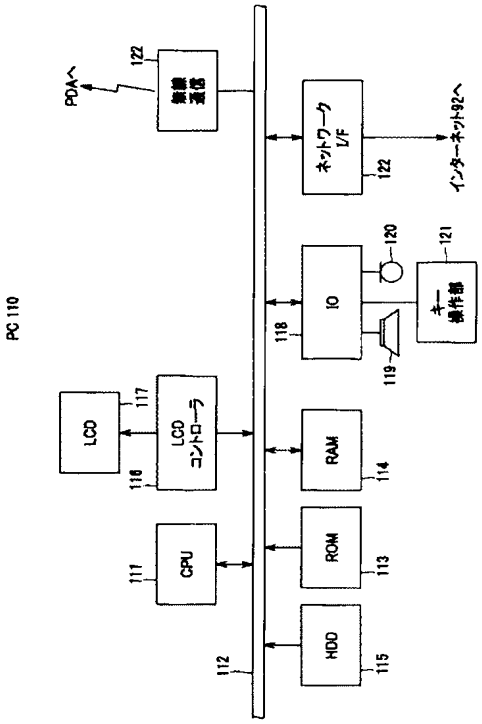
【図８】


チャージ出力
1
ブロードキャスト
N
スタンバイ
81
充電器→チャージ
2
1
N
認証要求
82
充電器のアドレスは接続されて1周期以上信号を監視すれば
自分のアドレスがわかる。
チャージ→充電器(1)
1
2
N
ID要求
83
充電器→チャージ
2
1
N
ID出力
84
チャージ→充電器
1
2
N
ID有効
85

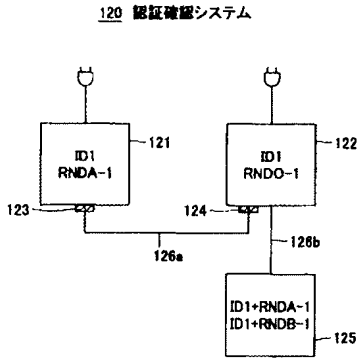
【図９】



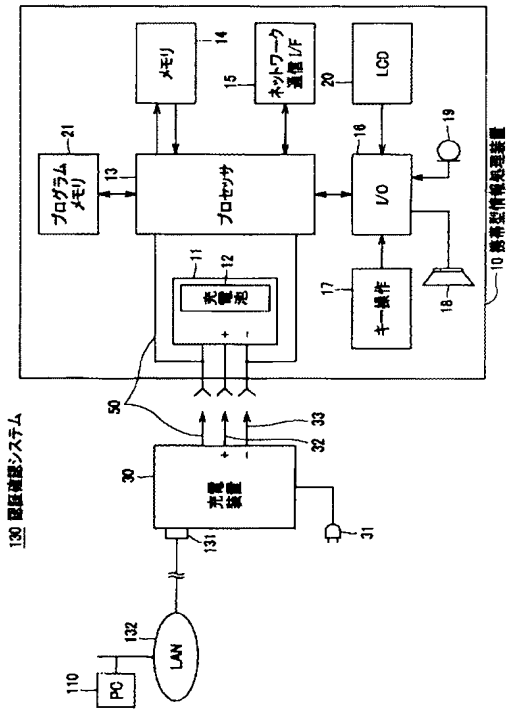
【図１０】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.[7]	F I		テーマコード（参考）
Ｈ０４Ｑ　7/38	Ｈ０４Ｍ	1/725	
	Ｈ０４Ｂ	7/26　１０９Ｓ	
	Ｈ０４Ｂ	7/26　Ｙ	

Ｆターム(参考) 5K027 AA11 BB09 GG04 GG08
5K067 AA32 BB04 DD17 EE02 FF02 FF07 HH22 HH23 HH36 KK06